# Quantum key distribution devices: How to make them and how to break them

by

Sarah Kaiser

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

Waterloo, Ontario, Canada, 2016

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

As more aspects of modern society depend on digital communication, we increasingly rely on infrastructure that ensures the privacy and security of this communication. Classically, this has been provided by cryptographic protocols such as public-key encryption, in which secrets called keys are exchanged between different parties to enable secure communication. The rapid development of quantum algorithms which violate the assumptions of these protocols, however, poses a security challenge to modern cryptography.

Quantum resources can also be used to strengthen cryptographic security, particularly the security of key exchange protocols. This approach, Quantum Key Distribution (QKD), can be implemented by encoding in quantum systems such as single photons sent through free-space or a fiber. Fiber based QKD devices are already commercially available, but are fundamentally limited to distributing keys over a few hundred kilometers. To address this distance limitation, research QKD systems are being developed to exchange keys through free-space to satellites. This work considers practical challenges to building and testing both types of QKD devices.

Firstly, we consider modeling and mission analysis for airborne demonstrations of QKD to stratospheric balloons and aircraft to simulate a satellite. Based on the mission parameters available for both platforms, we found aircraft platforms were more promising for testing prototype QKD satellite systems. We developed a mission planning tool to help design the flight geometries for testing the device.

Next, we developed three new components for a QKD satellite prototype. The requirements for electro-optical devices in orbit are very different from lab environments, mandating new approaches to designing QKD devices. We developed a quad single photon avalanche photodiode (SPAD) detector package to meet the requirements for free-space links to low earth orbit. Moreover, we designed and built optical systems for analyzing the polarization of photons and an adaptive optics unit to increase the efficiency of collecting the encoded photons. All three devices were tested in conditions that simulated the time and loss of a satellite pass.

Finally, we demonstrated a laser damage attack on a live commercial QKD system. Our attack injected additional optical power into the sender device to modify security-critical components. Specifically, our attack damaged the PIN diodes which monitor the encoded photon number, reducing their sensitivity or completely blinding them. Our damage could compromise the entire key, and was performed during system operation while raising no alarms.

In summary, this work shows the trade-offs of testing QKD payloads on different airborne platforms, develops components for a satellite QKD payload, and demonstrates a security vulnerability in a commercial QKD system that can fully compromise the key. These results help address practical challenges to building QKD devices, improving the security of modern cryptography.

**Acknowledgments**

I would like to thank no one more for helping me get this far than Chris. He believed in me when I didn't, and was always there to listen and advise.

Thanks to my family who has put up with all of my adopted Canadian-isms, and supported me in whatever I wanted to do. I love you guys so much.

Thanks to my supervisor, Thomas Jennewein and my group members for all their hard work.

There are so many wonderful people at IQC and in Waterloo that were there to help, discuss, and support at every turn: Olivia Di Matteo, Catherine Holloway, John Doucette, Alan Tsang, Carolyn Earnest, Emma McKay, Allison Sachs, Deborah Santiago, Aimee Gunther, Josh Combes, Jonah Miller, Alexandra Fresch, Yuval Sanders, Electra Eleftheriadou, Katanya Kuntz, Angela Olano, Jodi Szimanski, Jennifer Reid. There are so many more I missed and I will miss all ya'll.

I would also like to acknowledge my Mike and Ophelia Lazaridis fellowship as well as Cryptoworks21 for funding support.

A special thanks to those that helped make this a readable document: Olivia Di Matteo, Chris Granade, and Mom.

## Dedication

This is dedicated to the one I love, my dear Chris. Enjoy your burrito front dear ♡.

# Table of Contents

# List of Tables

# List of Figures

# Chapter 1

# Introduction

> Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say.
>
> Edward Snowden

## 1.1 Why is information security important?

We have grown up with spy stories of stolen microfilm and secret base plans that when the adversary gets hold of them, bad[1] things happen. Our cultural narrative has many stories like this about secrets and information security. Accordingly, with the huge shifts in the technology that we use to protect our security this narrative also must change. No longer is everything stored in a secret locked box or drawer, nor is it transported in briefcases handcuffed to a messenger's wrist. We felt secure depositing our valuables in safes in banks, knowing that there was insurance and a lot of metal protecting our stuff. We still as a society seem to be trying to apply these well-known and primarily physical concepts to the now drastically different modalities of security, often with catastrophic consequences. There are many modern aspects to information security, but we will focus on cryptography in this work.

Cryptography is often thought to just serve the purpose of transmitting and storing secrets. There are many different tasks that cryptography is used for, which are now an

[1] Well a matter of perspective, see examples of good outcomes for stolen goods: [1, 2, 3]

integral part of our society. These include tasks like generating randomness, certifying a party in a communication protocol, establishing a secret key between parties, and actual encryption of messages. These tasks are ubiquitous in modern life and to illustrate this, let's look at an example.

Consider the process by which a client logs in online to their bank account and pays a bill. When the clients browser reaches out to the bank server address, it should really verify the identity of the "bank". This task is known as certification and requires cryptographic signatures. These are often published by some "certification authority" who verifies that the signature was given to them from the correct party. You can inspect these certificates yourself by clicking on a lock or similar icon in the address bar of your browser [4, 5]. This is not entirely the whole picture as there is more than just the browser and the bank in the chain of trust. The certification authorities certify other certificate authorities and there are many levels to this before you start by trusting a link.

When the customer sets up the account, there is often a password given in person or mailed to them by the bank. These initial account passwords are often (and should be) random sequences of characters or symbols that the bank allows in the password. This task incorporates two important tasks of cryptography, generating secure randomness for the initial password, and getting the password to the customer. Generating cryptographically secure pseudorandom numbers is a very extensively studied task with detailed standards [6, 7]. This is a incredibly security critical task because in almost all protocols if an adversary has the same initial randomness (or key) then they can recover whatever was encrypted or stored. Unless the bank uses a specialized physical device to generate true randomness (like [8, 9]), randomness generated by software is only considered pseudorandom because it is produced by a deterministic process [10].

Once a random key is generated, how can it be shared to all the parties wanting to use it? If you happened to be at the bank when they generated the key, they might just write it down on a post-it for you or have you immediately use it to set a new password on a computer at the bank. However, if the parties needing to share the key are spatially separated then how can this be done? Exchanging the key is also a security critical process, and the task we look to add quantum resources to make it more secure. Classically, key exchange can be done by any number of certified algorithms like Diffie-Hellman [11] or various public key schemes [12] which also facilitate certification protocols. Just like in the movies, the most secure way is to do this physically, in person so that there is no chance for the key to be intercepted.

After the browser is sure that it is talking to the bank server, then the user can sign into their account. Passwords are useless if the computer just sent what the user typed, in plain

text. Then anyone monitoring the communication from machine to machine could easily get the user password. What actually happens is that a cryptographic hash of the password and user name is sent. A cryptographic hash function (or trap door function) is a way of taking some piece of information, scrambling and condensing it down to a smaller, fixed-length piece of information. Critically, this process must be extreamly computationally difficult to reverse and obtain the original information. An important feature of cryptographic hashs is that when very similar messages are scrambled, the shorter information pieces are not similar at all. This basically gives a way of uniquely correlating the shorter secret to the longer secret so that the longer secret is not compromised.

The last and most ubiquitous task of cryptography is encrypting messages. Say you have a question for your bank and you decide to send them a message using the "secure" messaging service on their website. The message you type in (just like your password) is called the plain text. Then some algorithm follows a set of steps to scramble the plain text with the key that was established between your computer and the bank server. This scrambled message is called the ciphertext and should not be readable or decodable by anyone who doesn't have the key that it was encoded with. The most secure way to do this scrambling is called one-time pad or Vernam cypher, which uses a key as long as the message (in binary representation) and bitwise add the plain text and key together [13, 14]. Once the ciphertext is generated, then text can be sent on public channels to the other party who then just bitwise adds the key again to retrieve the plain text of the message.

The advent of information that is stored electronically has opened up a whole new regime of ways to not only protect but also lose control of our personal information. There is an immense list of ways cryptographic protocols have failed, a few of which will be mentioned here. A recent compromise that has had wide reaching consequences is called BadUSB [15]. This vulnerability operates by hiding in the firmware for USB devices and is silently executed when plugged in to any computer. This can then install malicious code on the computer in an undetectable manner, simply from plugging it into a machine. An adversary using BadUSB relies on compromised hardware to exploit the device.

Another example is an exploit called Heartbleed [16] that is a compromise of OpenSSL cryptographic software library. This weakness allows for stealing information protected by the the lowest layer of internet security, called secure sockets layer (SSL). Heartbleed was a particularly bad vulnerability because it was in a very popular cryptographic library for a very long time, greatly increasing the number of systems effected. An adversary exploiting the Heartbleed weakness uses a mistake in the code implementing cryptographic algorithms.

Just like these examples of vulnerabilities to classical cryptographic protocols and devices, quantum protocols for key distribution will also have vulnerabilities which are ex-

amined in subsection 1.4.4.

### 1.1.1 How is quantum technology changing the status quo?

Just like security had been through a renaissance thanks to new technologies, computational resources are also changing thanks to quantum resources. This implies we should review our information security as well. As we have looked at already, most modern cryptography schemes rely on what is called *computational security* [17]. These schemes can be proven secure if and only if there are strong assumptions on the resources of an adversary (computing power or time). This is often compared to *information theoretic* security which allows adversaries unlimited computing power, and remain provably secure. While there are a few classical information theoretic protocols [18, 19], the use of quantum resources adds more protocols with this security guarantee. The guarantee is of course subject to the correctness of quantum mechanics, and if that does not hold we have bigger problems than cryptography.

The use of quantum resources in a protocol generally leads it to being called quantum cryptography, but this is not entirely clear. So far quantum resources are only used as parts of other protocols achieving tasks like key exchange but not actually the encryption of the message itself. No messages are sent with quantum systems, they are encoded with classical algorithms like one-time pad [14] and the key used for the algorithm was generated by quantum resources. Examples of the protocols that use quantum resources are called: Quantum Key Distribution (QKD) [20] and bit commitment [21]. Each of these address different cryptographic tasks, and can be used in combination with classical protocols to provide stronger cryptography. The main protocols that will be considered here is Quantum Key Distribution.

## 1.2 How can quantum information be sent with photons?

There are many different physical systems with quantum properties that are being explored for quantum computing and communication applications: N-V centers [22, 23], super conductors [24, 25, 26], and quantum dots [27, 28, 29] just to name a few. While each have advantages and disadvantages for various applications, photons are the preferred choice for quantum communication protocols as they are the easiest system to send physically between parties. Two-level photonic systems, or photonic qubits [30, 31], can be created

with a few different degrees of freedom that photons have. The most common is the polarization of the electric field of the photon, but the phase [32, 33], arrival time of the photon [34, 35], frequency [36], and spatial mode [37] or combinations of any of these [38, 39] can also be used to encode information. We will now describe some of the basic mathematical tools to describe the photonic qubits.

### 1.2.1 Operators

Creation and annihilation operators are common tools for describing quantum harmonic oscillators and other quantum systems [40]. In our application here they will represent adding and removing photons from a system. Let's start with time independent Schrödinger equation for a one-dimensional quantum harmonic oscillator [41]:

$$E_n\psi_n = \hat{H}\psi_n = \hbar\omega\left(\hat{a}^\dagger\hat{a} + \frac{1}{2}\right)\psi_n \tag{1.1}$$

where $\omega$ is the oscillator frequency, and $\hat{a}^\dagger$ is defined at the creation operator and $\hat{a}$ is defined as the annihilation operator. A mode is defined as a possible wavefunction that is a solution to this equation.

These operators are not Hermitian and have the commutation relation $\left[\hat{a}, \hat{a}^\dagger\right] = 1$.

#### Number operator

The number operator is defined as $\hat{n} \equiv \hat{a}^\dagger\hat{a}$. This is a useful operator as it helps define Fock states.

#### Fock States

Fock states are eigenstates of the number operator $\hat{n}$. The number operator tells us about how many photons are in a particular mode of a field, so Fock state states are usually labeled by integers $|0\rangle, |1\rangle, |2\rangle \ldots$ representing how many photons are in a mode. The creation operator and annihilation operator operators are used to define the number operator so it can be useful to see how they interact with Fock states:

$$\hat{a}\,|n\rangle = \sqrt{n}\,|n-1\rangle \tag{1.2}$$

$$\hat{a}^\dagger\,|n\rangle = \sqrt{n+1}\,|n+1\rangle \tag{1.3}$$

We can see that Fock state are eigenstates of $\hat{a}^\dagger$ and $\hat{a}$. Now, there is not really a physical meaning to $|n\rangle$ when $n < 0$ so what happens when $\hat{n}|0\rangle$? The energy of a harmonic oscillator must always be positive, and the lowest energy is in fact $\frac{1}{2}\hbar\omega$ for $n = 0$. The energy of a state lower than the ground state should be 0:

$$0 = \hat{H}(\hat{a}|0\rangle) = \tag{1.4}$$

$$\left(\hat{a}^\dagger\hat{a} + \frac{1}{2}\right)(\hat{a}|0\rangle) \tag{1.5}$$

$$\tag{1.6}$$

The only way the above relation is greater than or equal to $\frac{1}{2}\hbar\omega$, is if $\hat{a}|0\rangle = 0$.

Other useful properties of the Fock states is that they are orthonormal, that is $\langle n|m\rangle = \delta_{nm}$. Additionally they are a complete basis, that is to say

$$\sum_{n=0}^{\infty} |n\rangle\langle n| = 1 \tag{1.7}$$

These properties make Fock states a very convenient basis for quantum optics, and is one of the most frequently used.

### Coherent States

Coherent states, also known as Glauber states, are defined as eigenstates of the annihilation operator.

$$\hat{a}|\alpha\rangle = \alpha|\alpha\rangle \tag{1.8}$$

These states are most commonly used to describe laser light, which is abundant in experimental labs. As was noted before, the Fock states are a complete basis so coherent states can be written in that basis:

$$|\alpha\rangle = \exp\left[-\frac{1}{2}|\alpha|^2\right]\sum_{n=0}^{\infty}\frac{\alpha^n}{\sqrt{n!}}|n\rangle \tag{1.9}$$

### Density matrices

Quantum systems are described by Hilbert spaces ($\mathcal{H}$), and a quantum state is described by an operator acting on that Hilbert space. Density matrices $\rho$ are defined as any normalized positive semidefinite operator and correspond to a valid physical state of a quantum

system. Quantum states with a two-dimensional Hilbert space are known as qubits. Density matrices are important to QKD security proofs as they can be used to describe the state shared by all parties including an eavesdropper.

### 1.2.2 Quantum optical channels

QKD requires an optical channel between Alice and Bob to exchange the photons they encode with their key. There are two media for these channels, free-space or fiber optical cables. Free-space link systems are the focus of chapter 2 and chapter 3, while chapter 4 deals with fiber channels.

#### Free-space quantum channels

A free-space link could be through air between two devices in the same lab, or through the entire atmosphere from the ground to a satellite. Alice and Bob are usually concerned about knowing one primary parameter about this channel when doing a QKD protocol: loss. This can depend on what degree of freedom they are encoding in their photons, but for the rest of the systems discussed in this work, loss is the primary descriptor for the channel. The most common way to model loss is to use a perfect channel and beamsplitters that deflect out of the channel the same percentage of photons that are realistically lost.

When a photon is traveling through the atmosphere from a party on the ground to a party in space, it can be lost in five primary ways [42]:

- diffraction,
- turbulence,
- pointing of the optical path,
- absorption by elements in the atmosphere, and
- type of collection optics and the efficiency of the receiver components.

We assume here both the sender and receiver are using telescopes as respectively the last and first optical element of their devices. Additionally, the contributions of each of these effects can be different depending on whether the source is on the ground (uplink) or in space (downlink).

Diffraction is a fundamental behavior for Gaussian beams, and the effects can be minimized by using larger beam diameters which in our case means larger transmitter telescopes.

There is no way to fully characterize the chaotic process that is the air turbulence in the atmosphere but we can bound how badly it will affect the beam. Localized changes in the index of refraction of the path define the process of turbulence on an optical path. Turbulence can cause the optical path to wander and broaden, as well intensity fluctuations of the beam. Downlinks have reduced loss from turbulence due to the fact that the atmospheric density near the source is much lower than an uplink, and effects like beam wander are more impactful closer to the source. Conveniently, while stable intensity, spatial modes, or phases are heavily affected by turbulence, polarization is not [43]. It is for these reasons free-space QKD will often us polarization (or time bin) encoding for the qubits.

Loss due to pointing telescopes is very classical problem, which is solved all the time for many applications like light detection and ranging (LIDAR) and astronomy. One needs very stable and fine control of the motors moving the telescopes and some sort of active feedback to optimize the pointing. Pointing of the source telescope is more critical than the receiver because the beam diameter is smaller and a small error has the whole length of the channel to propagate and expand.

There are many different species of gas in the atmosphere and thus many possible optical frequencies that could be absorbed or scattered. Modeling was done [42] to find windows in the optical spectrum to try and minimize the chance that the signal wavelength would be absorbed in the atmosphere. It was found that generally the longer the wavelength (even from visible into the near infrared) the better the transmission. However, other hardware efficiency constraints must be considered when selecting a signal wavelength.

Lastly, losses that are considered part of the channel but not exactly in the channel are those of the hardware used to collect photons from the channel. Generally speaking, this means things like detector efficiency, the field-of-view (FOV) and diameter of the telescope, and efficiency of other optical elements that come after the telescope but before the detectors. One point to note about the telescope design is some telescopes have reflective elements, and unless specially coated this will distort polarization states [44].

### Fiber optical quantum channels

Fiber optic cables represent a much more deterministic link between Alice and Bob, but have much higher average loss per unit distance (relative to a free-space link to space)

thereby limiting the distance over which fiber based QKD systems can be used. Again, we are concerned with the loss mechanisms, which for a glass medium are absorption and scattering [45]. These loss mechanisms hold for all waveguides, but here we are generally concerned with single mode telecommunication fiber (SMF28).

Scattering loss in a fiber is very easy to see, the light is only confined to the core of the fiber as long as it is totally internally reflected by the core-cladding boundary. This interface is not perfect and manufacturing defects, bad splices, or bad connectors can cause light to be scattered out of the core and lost to Alice and Bob.

Losses due to absorption are also easily motivated: Light can be absorbed by atoms in the glass directly or into a vibrational mode of the atomic lattice itself. Commercial fibers, especially for telecommunications already minimize these absorptions as much as possible in manufacturing so what loss to absorption remains is unavoidable.

### Photon encoding methods

Now that we have briefly addressed the channels that we will use to transmit photons, we can now talk about how we should encode our information on the photons. There are 3 primary degrees of freedom that are used to encode information on photons: arrival times (time-bin), polarization, and phase. For the fiber based channels phase and time-bins are better choices as glass is birefringent which will scramble polarization states sent through the channel. This can still be done with active stabilization of the polarization reference frames at both Alice and Bob, but this is difficult task and unnecessary if other degrees of freedom are chosen. There have been many successful demonstrations in fiber channels of time-bin [46, 47] and phase [33, 48] to list a few.

Free-space channels generally favor polarization encoding, as it is the least disturbed by transmission through the turbulent atmosphere[49]. This can be easily seen by looking at how the different encodings are measured. Both time-bin and phase require an interferometric measurements, which are significantly degraded when there are dispersive media in the channel. For time-bins, not only with the spatial modes of the two pulses be differently altered due to the time-dependent processes in the atmosphere, but the literal time of flight of each pulse can vary making it hard to interfere them. The dispersion arguments also hold for the phase encoding. Since we are most interested in free-space channels when building QKD systems, we will then look at encoding our bits in polarization.

## 1.3 Detection tools

There are many different technologies and methods for detecting single photons: photo multiplier tube (PMT), super-conducting detectors, and semiconductor photodiodes to name a few. Each type of device has different properties and operating conditions that inform which would be the best choice for a particular experiment. There are a few parameters used to describe these devices (from [50]):

- **Detection efficiency**: Detection efficiency is the ratio of detected photons to incident photons on a detector. It is comprised of 3 sub-quantities:

$$\eta_{DE} = \eta_{absorb}\ \eta_{QE}\ \eta_{threshold} \tag{1.10}$$

  $\eta_{absorb}$ is the efficiency with which the semiconductor can absorb the photon, $\eta_{QE}$ is the efficiency of the process that converts photons to electrons in the material, and $\eta_{threshold}$ is the efficiency that detector readout circuit registers detection events.

- **Dark count rate**: The dark count rate of a detector is the rate at which the device reports detection events when there was no input light. These counts have many causes, often thermal fluctuations in the detector material or readout electronics.

- **Afterpulsing**: Afterpulsing of detectors is when some time after a detection event, another false detection event is registered. This can be from charge trapping in a material during a detection event which via thermal processes later continues or restarts an event.

- **Timing jitter**: Timing jitter is a measure of the time correlation between the arrival of a photon to be detected and when the detection event is actually registered. It is usually stated as the full width half max (FWHM) of the distribution of delays from photon arrival to detection. The actual magnitude of the delay is often not an issue, it is the statistical fluctuation of the arrival times that can make precise timing of detector gating or subsequent operations conditional on detector outcome that are problematic.

- **Crosstalk**: Crosstalk and fill factor both refer mainly to devices with multiple active areas or pixels. Cross talk is when activity in one pixel or device influences other on the same chip or substrate.

- **Fill factor**: Fill factor is simply the ratio of active area to total illuminated area of a detector. This again is a parameter intended to describe arrayed devices.

- **Figure of merit**: Developed in [51], this measure uses the above properties which are most important to QKD to provide a way of comparing detector performance for quantum information experiments. It can be stated as $H = \eta/(D\Delta t)$, where $\eta$ is the detector efficiency, $D$ is the dark count rate, $\Delta t$ is the FWHM of the timing jitter distribution.

For the long-distance Quantum Key Distribution (QKD) demonstrations, the selected detector must be ruggedly packaged and usable outdoors as well as fit in a small volume and have low power consumption. These requirements quickly rule out superconductor detector devices, which require vacuum and often cryogenic temperatures. Neither of these operating conditions are easily obtainable in small physical or power form factors. That leaves semiconductors and photo multiplier tubes.

Photo multiplier tubes (PMTs) have been in use longer than semiconductor devices and offer many benefits including large active areas ($\sim$ 1cm$^2$) and low timing jitter. The wavelength sensitivity for these devices is greatest in the visible range, and have detection efficiencies of up to 40% in this range. However this relatively high efficiency drops off quickly at the red end of visible and is negligible in near infrared. It was shown in previous studies [49] that the optimal wavelengths for space quantum links is in the $670 - 780$ nm range which would not be optimal for PMT. By ruling out the other detector options we are left with semiconductor devices as candidate technologies for free-space and satellite QKD.

Apart from the lack of other candidates, there are some good reasons to use semiconductor single photon detector devices. Silicon-based avalanche photodiodes (APDs) are sensitive in the visible and near-infrared (up to 1100 nm) wavelength range, with peak detection efficiencies of $50-60\%$ [50]. They already are easy to manufacture in small physical packages and operate with relatively low power. There are other semiconductors that could and have been used to make single photon detectors, but due to current semiconductor materials processing techniques and sample purities, silicon has the best characteristics. Indium gallium arsenide (InGaAs) is another common material that has even better infrared sensitivity but lacks in other aspects because there is not a large industry backing the development of fabrication techniques. The next section will describe how APD work as well as common readout circuits for the devices.

### 1.3.1 Operation of semiconductor based single-photon detectors

The avalanche photodiodes (APDs) build on a long history of semiconductor devices. Like many semiconductor devices, they can be made from different materials and benefit from

well developed fabrication techniques. APD rely on a p/n junction that has material doped such that there is an excess of holes (or a spot lacking an electron) in the p half and an excess of electrons in the n half. This is the same basic makeup of any semiconductor diode. What allows for the "avalanche" behavior is reverse biasing the junction (see Figure 1.1).

In this scenario, normally bound electrons or holes are more likely to be kicked free of their bonds by thermal fluctuations or excitation. It is the excitation case, where an incident photon absorbed in the material then liberates an electron hole pair. The free electron and hole move toward the positive and negative biased sides of the diode respectively. As they move through the material they are accelerated by the electric field created by the voltage across the diode. This can cause more collisions (via impact ionization) and free more electron hole pairs. This process can snowball and lead to a measurable current across the device, known as an avalanche. How this current is measured is critical to the performance of the device, and will be looked at in Section 1.3.1.

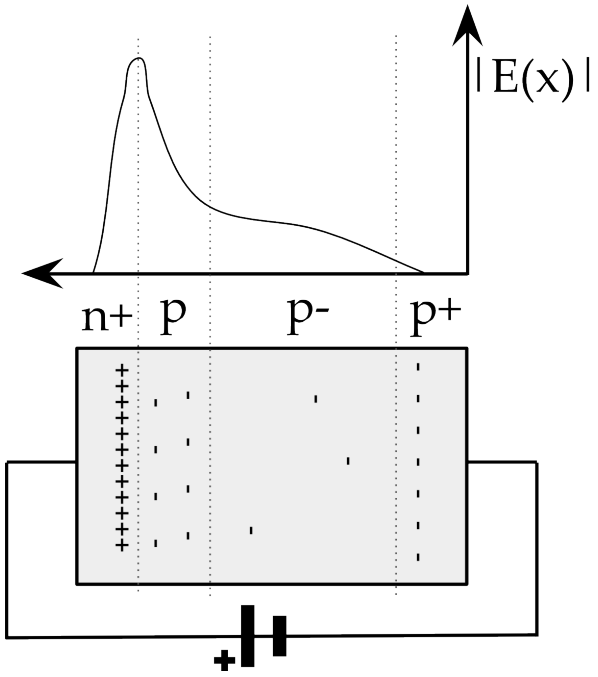



Figure 1.1: Diagram of the junction of an APD [50]. The dopents in the material layers help shape the electric potential in each region to help reduce the delay of avalanche propagation.

The amount of reverse bias on the devices can have an important effect on the behavior of the avalanche. The devices have what is called a breakdown voltage which when reversed

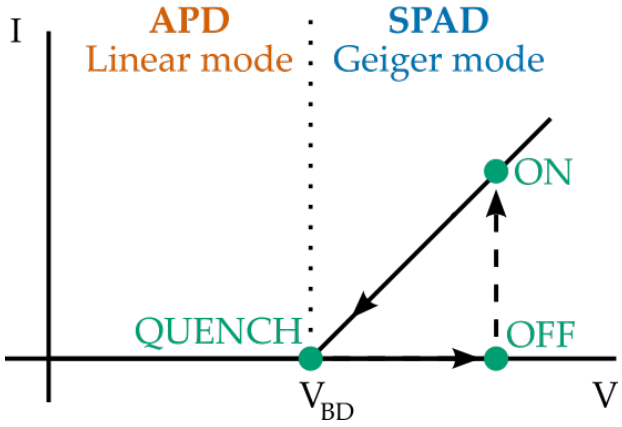



Figure 1.2: Plot of a qualitative I-V curve for a APD. The dots indicate the three main states that the detector can be in: "Off" for when the detector is biased over breakdown voltage and is awaiting a incident photon, "On" for when a photon is absorbed, triggering an avalanche of electrons and a measurable current, and "Quenched" for when the current through the diode causes a voltage drop across the diode, reducing the bias voltage to the breakdown voltage level. When the diode becomes quenched, the current though the diode exponentially drops off and then the bias voltage across the diode builds up again to the "Off" state. This cycle is known as passive quenching 1.3.1.

biased above this value the device is called a single photon avalanche photodiode (SPAD), and is sensitive enough to detect single photons.

As can be seen in Figure 1.2, below the breakdown the device operates in "linear mode" in which the current across the junction is proportional to the incident optical power. Above the breakdown the device enters "Geiger mode" where there is so much potential across the device, the energy transfered from even a single photon can start an avalanche with a measurable current. Therefore, to be able to use the devices as single photon detectors, we bias the devices above the breakdown voltage. Deciding how much to bias the device over the breakdown voltage can be highly dependent on the electronics that detect the avalanche current. Additionally, the avalanche current will be self sustaining in Geiger mode unless quenched by the readout circuit. This quenching of the avalanche can be achieved by either passive or active components as discussed in Section 1.3.1.

As mentioned previously there are various materials that the diodes can be made out of that vary their performance. The common materials currently used for SPAD devices are silicon and Indium gallium arsenide (InGaAs). Silicon is a very popular choice since it has been used in the semiconductor industry for a long time and the protocols for processing and

fabricating the material with low contamination levels. However, the absorption of Silicon while good across the visible spectrum, falls off quickly for the infrared [52]. For SPADs that perform well in the infrared, especially at common telecommunication wavelengths (1310 & 1550 nm) InGaAs has some of the best performance of commercially used materials currently [53, 54, 55].

In principal, the performances of these materials could be comparable for their different sensitivity regimes, but in general pratice InGaAs is always a bit worse. This is because material impurities or defects that are a product of the device fabrication are more prevalent in InGaAs. There was not as much market for InGaAs APD historically, so the fabrication technology for the material is not as advanced as that of silicon. This performance gap is expected to shrink as there is more demand for telecommunication optical devices [50].

There are many different commercial SPAD devices with varying performances. The main differentiator of these devices is the readout circuit, which includes avalanche detection and quenching components. There are many different approaches for quenching components in the readout circuits, but the main one discussed here is passive quenching. More details on other variants can be found in [50].

### Passive quenching

Passive quenching of an SPAD relies on the fact that if there is avalanche current through the device, then there will be a voltage drop across it since there is some effective internal resistance in the diode. This then reduces the reverse bias across the device until it is below breakdown and there is insufficient electric field intensities to sustain the avalanche. This is identical to the sequence of states described in Figure 1.2. To see more details on how this works, see Figure 1.3 for a passive, current-mode readout circuit and Figure 1.4 for a model of how the avalanche in the diode works [56].

The bias voltage for the diode is applied across three elements: $R_L$ a large ballast resistor, the APD, and a small resistor $R_S$ used to see the avalanche current. The comparator then monitors the voltage drop across $R_S$ which spikes rapidly when the avalanche starts. Since the comparator looks at a voltage spike due to the spike in the avalanche current, this is called current-mode detection of an APD. There is a threshold set then in the comparator that can be varied to change the performance of the detector. The lower it is set, the lower the timing jitter of the detector, as it catches the rising edge of the current spike at a more reliable place. The trade-off is then the detector is more likely to trigger on noise in the signal. The comparator then generates a digital signal (transistor-transistor logic (TTL) or similar) that can be sent to timing electronics to record the exact time of the

avalanche event. The recovery time for a passively quenched device is usually on the order of μs so if faster detection rates are needed, then an active quenching system is required [57].

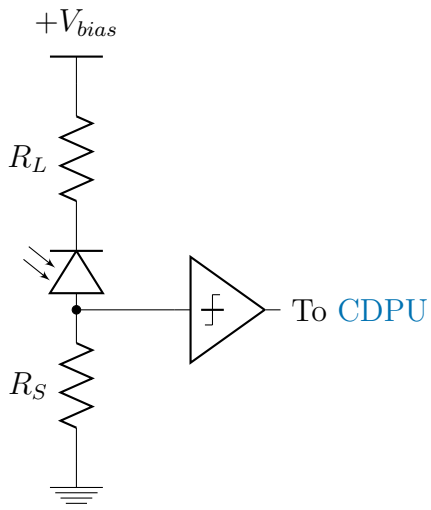



Figure 1.3: Equivalent circuit of the current-mode passive quenching circuit. The avalanche signal is sensed by the comparator that produces a standard signal for pulse counting and timing.

Now lets walk through what happens to the diode at a slightly more detailed level (see Figure 1.4). The dashed box in the figure represents the equivalent circuit for the APD in the context of the rest of the passive, current-mode readout circuit. The avalanche is started when switch $S$ is closed. The current through the diode is then given as a function of the time-dependent voltage above breakdown:

$$I_{\text{diode}} = \frac{V_{\text{over}}(t)}{R_d} \tag{1.11}$$

The avalanche will continue as long as the two capacitances are discharging, $C_s$ (stray capacitance) and $C_d$ (junction capacitance). The time to discharge the capacitances and

the steady state current is given as:

$$t_{\text{quench}} = (C_d + C_s) \cdot \frac{R_d R_L}{R_d + R_L} \tag{1.12}$$

$$\cong (C_d + C_s) R_d \quad \text{if } R_L \gg R_d \tag{1.13}$$

$$I_{\text{diode-steady}} = \frac{V_{\text{over}}(t)}{R_d + R_L} \tag{1.14}$$

$$\cong \frac{V_{\text{over}}(t)}{R_L} \quad \text{if } R_L \gg R_d \tag{1.15}$$

$$\tag{1.16}$$

As the carriers in the number of carriers in the semiconductor starts to decrease and the avalanche flow reduces, $V_{\text{over}}(t)$ and $I_{\text{diode-steady}}$ asymptomatically approach 0. However this behavior is interrupted as there is a critical current that must be maintained through the diode to keep the switch closed. When it is reached, the switch abruptly opens and then there is 0 current through the diode and the voltage across the diode can charge the capacitors back up again. The recharge time is given by:

$$t_{\text{recovery}} = (C_d + C_s) R_L \tag{1.17}$$

We can see then that the selection of the load resistor $R_L$ has a significant effect on the recharge time, and hence the timing jitter of the device. The other two capacitances are tiny and not really controllable, as they are generally a function of the device and circuit manufacture.

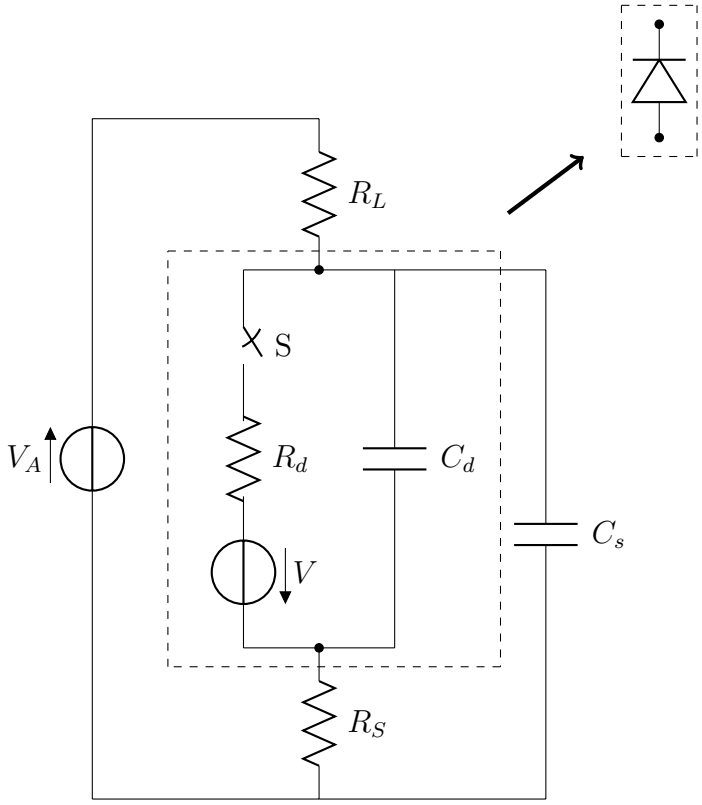



Figure 1.4: Equivalent circuit of the current-mode passive quenching circuit [56]. The avalanche signal is sensed by the comparator (see 1.3) that produces a standard signal for pulse counting and timing.

## 1.4 Security of Quantum Key Distribution

QKD promises that two parties trying to communicate, let's canonically call them Alice and Bob, will be able tell if a third party (called an eavesdropper or Eve) has interfered with or seen a key they are trying to share. It does not promise that a key can be established, only that if a key bits are shared between Alice and Bob that they have a kind of "tamper-proof seal" on them. Just like when you buy a jar of peanut butter and you see the seal on the jar is broken, key bits that have had this seal broken should be thrown out. This is essentially the benefit that quantum systems afford to the key exchange process.

Most QKD protocols usually require 2 main resources between Alice and Bob: a quantum channel and an authenticated classical channel. However, Alice and Bob are only

looking for the classical key bits that were encoded and sent on the quantum channel, so they can be modeled as each having a classical bit register and then there is some register that an eavesdropper has access to. The classical registers can be embedded in a quantum register by mapping the classical readouts to orthogonal basis states. The joint state between Alice, Bob, and the eavesdropper can be written as [58]:

$$\rho_{\mathrm{ABE}} = \sum_{K} \sum_{K'} p(K, K') \left|K\right\rangle \left\langle K\right|_{\mathrm{A}} \otimes \left|K'\right\rangle \left\langle K'\right|_{\mathrm{B}} \otimes \rho_{\mathrm{E}}^{(K,K')} \tag{1.18}$$

$K$ and $K'$ are the index of the states of the classical registers that Alice and Bob hold, and $\rho_{\mathrm{E}}^{(K,K')}$ is a fully quantum state that is correlated to the state of the of both classical registers (ideally from the eavesdropper's perspective). $p(K, K')$ is the joint probability distribution for the classical registers. In an ideal world from Alice and Bob's perspective their registers should agree $K = K'$, and should be uniformly distributed over all possible keys $p(K, K') = \frac{1}{|\mathcal{K}|}\delta_{K,K'}$. Also, Alice and Bob do not want the eavesdropper correlated with their registers so $\rho_{\mathrm{E}}^{(K,K')} \equiv \rho_{\mathrm{E}}$ for all $K, K'$. Then optimally from Alice and Bob's perspective:

$$\rho_{\mathrm{ABE}}^{\mathrm{ideal}} = \frac{1}{|\mathcal{K}|} \left( \sum_{K} \left|K\right\rangle \left\langle K\right|_{\mathrm{A}} \otimes \left|K\right\rangle \left\langle K\right|_{\mathrm{B}} \right) \otimes \rho_{\mathrm{E}} \tag{1.19}$$

A QKD protocol uses measurements on the quantum states sent to verify if they are in the ideal state of (1.19). If that can be proven, we know Eve can know nothing about the key registers of Alice and Bob as she is completely uncorrelated from their joint state.

Realistically, no party will have perfect quantum states due to losses so we have to slightly change the language about the security claimed from a particular protocol. We define a protocol as $\epsilon$ secure if after the execution of the protocol there exists a density matrix $\rho_{\mathrm{ABE}}^{\mathrm{ideal}}$ such that [59]:

$$\frac{1}{2}||\rho_{\mathrm{ABE}} - \rho_{\mathrm{ABE}}^{\mathrm{ideal}}||_1 < \epsilon \tag{1.20}$$

where $||\ ||_1$ is the trace norm. The trace norm here is used mostly by convention for state distinguishably tasks that are made easy with this particular distance measure [60]. $\epsilon$ can be interpreted as the probability that the protocol does not abort, and the eavesdropper will have some knowledge of the key. Defining the security criterion like this provides the benefit of making it composable [61]. This property allows multiple composably secure protocols to be combined and maintain the same security guarantee.

There are many variants of protocols for QKD and most fall into two general categories: entanglement based and prepare and measure. Each of these categories rely on different principals of quantum mechanics to prove the security.

Entanglement based protocols use as the name implies shared entanglement or correlations that ensure that Alice and Bob have correlated measurement outcomes to create the key. The prepare and measure protocols use the fact that non-orthogonal states cannot be perfectly distinguished [62], and that cloning of quantum states is forbidden [62]. These two properties of quantum mechanics combine to ensure an eavesdropper can only gain information about the key probabilistically.

The protocol that we will be looking at in this work which was first complete proposal for QKD was Bennett Brassard 1984 [20], though the first mention of a protocol was in [63]. The protocol (referred to as BB84), is a prepare and measure protocol that is implemented with photons.

### 1.4.1 Requirements

QKD protocols have conditions for the environment in which they are used, to ensure the security proofs can be applied. There is a lot of progress to expand the security proofs to relax or remove these conditions [64], the most extreme of which are called device independent quantum key distribution (DIQKD) [65, 66, 67]. These protocols make no assumptions about the equipment used to implement the protocol, but have very impractical key rates (with current technology). Since there are many different hardware implementation options this approach can be useful for specific use cases, but does not seem likely to incorporate *all* aspects of real hardware in the security proof. Let's look now at some of the basic conditions for these protocols.

The first and most obvious requirement are that an eavesdropper is not allowed access to the physical devices or labs that Alice and Bob are operating in. This is a standard assumption even classical cryptographic schemes. Similarly, the randomness used in the protocol for the key bit selection, basis selection, and other parts of the classical communication must not be compromised. The easiest way to do this is to have quantum random number generator (QRNG). For a review on QRNGs see [68].

Another requirement for QKD systems is the classical communication channel between Alice and Bob is authenticated. This means that Alice and Bob must start the QKD protocol with some shared key or secret already. Therefore QKD is only a key expansion protocol in actuality as it cannot be started without some shared key already. The reason for this requirement can be seen obviously from man in the middle attacks (see

subsection 1.4.4). If the classical channel was not authenticated, then another party like an eavesdropper could intercept the classical messages to and from Alice and pretend to be Bob. Though this may be seen as a weakness of the protocol, most classical crypto relies on a chain of trust that at some point has to start somewhere. So this concept of having some prior secret or trust for a protocol is a common piece of classical cryptography as well.

Lastly once the key is generated from a QKD protocol, it should be used with perfect security protocols like one-time pad scheme. Security for protocols are often only as secure as the weakest component, and thus a final statement about the security of a protocol is only as strong as the weakest statement for a component. If a quantum generated key is used in an insecure protocol after, the security from the key is useless.

### 1.4.2 BB84 Protocol

To review, the resources necessary for this protocol are: an optical channel to send the encoded quantum systems (which we will assume here is noisy, i.e. that there is extra light not part of the protocol in the channel), and an authenticated classical channel. Eve is allowed full access to both, but since the classical channel is authenticated she cannot modify any of the messages there. The BB84 protocol has two major phases, the quantum phase and the classical phase.

**Quantum phase**

In the Quantum phase of BB84 Alice and Bob prepare, share, and measure encoded photons. There are many different degrees of freedom that can be used to encode information on photons, but the two most common are polarization and phase. Polarization is preferred for free-space quantum links (see 1.2.2), and phase for fiber links as the both experience minimal perturbation in the respective channels. For the description of the protocol, we will refer to polarization encoding, and the states indicating a physical orientation for the polarization: Horizontal (H), Vertical (V), Diagonal (D) and Anti-diagonal (A). Both parties at the end of this phase should have a series of binary bit values and a corresponding record of what basis that bit was prepared or measured in.

The first step of the protocol is Alice generates random numbers to decide on two settings per photon: the basis to encode in, and the bit value to be sent. The 4 possible states are:

$$|0\rangle = |H\rangle \quad (H/V \text{ basis}) \tag{1.21}$$
$$|1\rangle = |V\rangle \quad (H/V \text{ basis}) \tag{1.22}$$
$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |D\rangle \quad (D/A \text{ basis}) \tag{1.23}$$
$$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |A\rangle \quad (D/A \text{ basis}) \tag{1.24}$$

The reason for the two different bases will be discussed in subsection 1.4.3. Once she chooses one of these states, she prepares a photon in that state, records the state she prepared, and then sends the encoded single photon through the optical channel to Bob. Bob decided for each arriving photon independently which basis to measure it in (H/V or A/D). Bob then records his measurement outcomes and the basis he measured in.

**Classical Phase**

Once Alice and Bob both have a list of measurement values and bases associated with each photon, they proceed to the classical stage. Alice starts by announcing over the authenticate classical channel a subset of her measurement values and bases to announce to Bob and he responds publicly if they match what he had. This is called parameter estimation, and is the step where Alice and Bob are checking to see if they shared ideal states ((1.19)). After disclosing a certain number of measurements, they decide if they had matching outcomes and if so they proceed with the rest of the protocol. If they observe too many measurements not matching they abort the protocol.

Next, Alice and Bob announce the bases they each used to prepare or measure each remaining photon. They each then throw out measurements that they did not prepare/measure in the same basis. The measurements left at this stage are mapped to bit values (most simply H/D$\rightarrow$ 0,V/A$\rightarrow$ 1) and called the "sifted key".

Since it was assumed that the quantum channel has losses, at this point Alice and Bob perform a classical error correction algorithm to ensure that the remaining bits match. However, through this process small amounts of information about the sifted key must be leaked, necessitating the next step, privacy amplification. In this last step, all ways in which information about the key has potentially been leaked to Eve are estimated and the remaining error corrected key is scrambled and reduced in length. This statistically removes any information Eve may have about the key, and is done with what are called universal functions [69].

In Table 1.1, a sample exchange up to the sifting step is shown.

Table 1.1: Sample exchange of key bits in a BB84 protocol. The arrow directions map to the polarization states used to encode the bit/basis values

| Alice's random bit | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 |
|---|---|---|---|---|---|---|---|---|
| Alice's random sending basis | + | + | × | + | × | × | × | + |
| Photon polarization Alice sends | ↑ | → | ↘ | ↑ | ↘ | ↗ | ↗ | → |
| Bob's random measuring basis | + | × | × | × | + | × | + | + |
| Photon polarization Bob measures | ↑ | ↗ | ↘ | ↗ | → | ↗ | → | → |
| Shared secret key after sifting | 0 | | 1 | | | 0 | | 1 |

### 1.4.3 How do quantum resources guarantee security?

As we mentioned before there are two main categories of QKD protocols: entanglement based, and prepare and measure. First we will look at why entanglement based protocols like Ekert 1991 (E91) [70] work.

Consider an entangled source that produces a tripartite system, where two of the parts of qubits and distributed to Alice and Bob. We give the other part of the system to Eve, including the source itself. Now we know if we can show Alice and Bob's qubits are maximally entangled, then by the monogamy of entanglement [62] (If two qubits are maximally entangled they cannot be correlated at all with a third qubit), Eve is necessarily uncorrelated to Alice and Bob. Alice and Bob then each perform random measurements on qubits in random choices of the H/V or D/A basis. Let's say they reveal a subset of their measurements and bases and find that when they chose the same basis their measurements were always correlated and when they measured in different bases were completely uncorrelated. They only state that could explain this observation is the Bell state $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A |0\rangle_B + |1\rangle_A |1\rangle_B)$, which is a pure state that is maximally entangled and thus is uncorrelated with Eve's remaining state. This obviously assumes that the source is producing entangled states, which if it is not then it obviously cannot be used for this protocol. The state that is produced by an actual entangled source is then:

$$\rho_{\mathrm{ABE}}^{\mathrm{bell}} = |\phi^+\rangle \langle\phi^+| \otimes \rho_{\mathrm{E}} \tag{1.25}$$

Now let's look at the origin for the security of prepare and measure protocols like BB84,Bennett-Brassard-Mermin 1992 (BBM92)[71]. The general concept that secures these protocols is the fact that quantum states are non-deterministic, and when interacting with a state an eavesdropper must disrupt the state. The eavesdropper cannot clone the state, so they must interact with the actual states Alice is sending to Bob. Proving these

types of protocols is hard to do directly, but there is a handy trick called *source-replacement* [71] that basically allows prepare and measure protocols to use the security proofs from entanglement protocols.

The source-replacement technique describes Alice's state preparation step as an entangled source as opposed to a deterministic state generator. Alice generates bipartite states of the form:

$$|\Phi\rangle_{AS} = \sum_{x=1}^{n} \sqrt{p(x)}\, |i_x\rangle_A\, |\phi_x\rangle_S \tag{1.26}$$

where $|i_x\rangle$ is a set of orthonormal states in an n-dimensional Hilbert space, and she keeps system $A$ and sends system $S$ as the signal to Bob. Alice "prepares" state $|\phi_x\rangle$ with probability $\sqrt{p(x)}$ by doing a projective measurement on the $A$ system. Since she keeps system $A$ and it is unaffected by the action of the channel, Alice's preparation of the state commutes with the channel evolution. We are now back to trying to show that the tripartite state the Eve is allowed to create ($\rho_{\text{ABE}}$) in fact is of the form shown in (1.19).

### 1.4.4 Attacks on QKD

When implemented, QKD protocols can be implemented with polarization states, distributed phase references, or continuous variable optical modes. Each of these implementations can have benefits and drawbacks for the environment in which it is being used. Similarly they all have different kinds of attacks that they are vulnerable to. We will now discuss some of the more common attacks that specifically BB84 protocols are vulnerable to. Just like the classical cryptography, the source of the vulnerability can be in the hardware, software, or protocol level of the system.

If the attack is targeting the quantum signals traveling between Alice and Bob, there are a few ways an eavesdropper can structure their attack. These categorizations are motivated by the fact that some protocols have security proofs which can protect from some of these categories of attacks. The simplest (and weakest) is to target the qubits sent individually and attack each identically. A slightly stronger approach is to use a collective attack where Eve attaches a probe system to each signal and can do something with the probes after additional information is revealed. QKD was shown secure against collective attacks in 1998 [72]. The strongest type of attack an eavesdropper can use is a coherent attack where Eve is allowed a collective attack plus quantum operations on all of the probe states. There exist security proofs that guards against coherent attacks [73, 74], but technological limitations make this type of attack not currently practical. This is

mainly due to the fact that Eve would need quantum memories [75] and possibly quantum non-demolition measurements [76] both of which exist today in some capacity but need to improved greatly to enable practical attacks.

Though QKD is a relatively new technology, there is already a large body of work outlining the vulnerabilities that have been found in all parts of the QKD system. Hardware vulnerabilities like random number generation attacks [77, 78] or Trojan horse attacks [79, 80, 81] passively monitor Alice and Bob's devices, learning information about the key leaked through what are called side channels. These vulnerability are not captured in the security proofs as perfect device models leak no information while operating.

If all Eve wants to do is stop the QKD protocol, they can simply cut off the quantum channel between Alice and Bob called a denial of service attack [82]. There is no protection for this type of attack classically or with quantum resources, and is not considered further. Some other possible attacks are: the time shift attack [83], phase remapping attack [84], photon number splitting attack [85], and detector control attack [86] that served as the inspiration for chapter 4.

### Intercept-resend attack

In the intercept-resend attack [87], Eve takes the photons sent by Alice and acts as a copy of Bob to generate a key. Eve then uses a copy of Alice to send signals to the real Bob and try and get his measurements to mimic those made by Eve's fake Bob. This vulnerability is in the protocol level of the system, as no hardware or software components have to malfunction to permit this. An outline for this attack can be seen in Table 1.2. Eve will introduce errors in the sifted key 25% of the time because of the 50% of the time she guesses the wrong basis, 50% of Bob's random detections will turn out to be the right bit value. If Eve guesses the same basis as Alice and Bob, no errors are introduced. If Eve chooses the wrong basis, half of the time Bob will still randomly measure the correct outcome. Because Alice and Bob will announce their basis choices, Eve will get full information of half the key at the cost of introducing a 25% error rate.

By reducing the frequency of the attack then induces error rate can be reduced to more "normal" levels, and it is conceivable that if you have a 8% error rate, Eve may know up to 16% of the final key. However, this is in the average case, Eve could statistically introduce far fewer errors in the measurements and thus lead Alice and Bob to underestimate the potential knowledge that Eve has about the key. In this manner we see that an $\epsilon$ definition of security for QKD is needed, and described here [59]. The best way to counter this attack is to be extremely conservative with the parameter estimation and privacy amplification

Table 1.2: Table of sample outcomes of qubits prepared in a BB84 protocol that is subject to an intercept-resend attack. The arrow directions indicate the polarization of the photons. Note how Eve can only correctly learn the bit value if she measures in the same basis as Alice and Bob.

| 1.Alice's random bit | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 |
|---|---|---|---|---|---|---|---|---|
| 2.Alice's random sending basis | + | + | × | + | × | × | × | + |
| 3.Photon polarization Alice sends | ↑ | → | ↘ | ↑ | ↘ | ↗ | ↗ | → |
| 4.Eve's random measuring basis | + | × | + | + | × | + | × | + |
| 5.Polarization Eve measures and sends | ↑ | ↗ | → | ↑ | ↘ | → | ↗ | → |
| 6.Bob's random measuring basis | + | × | × | × | + | × | + | + |
| 7.Photon polarization Bob measures | ↑ | ↗ | ↗ | ↘ | → | ↗ | ↑ | → |
| Eve's shared secret key | 0 | | 0 | | | 0 | | 1 |
| Errors in Eve's key | ✓ | | X | | | ✓ | | ✓ |

steps of the protocol. The trade-off is then you need more measurements to get the same key rate because more will have to be revealed in the protocol.

Intercept-resend attacks seem similar to man-in-the-middle attacks [88] which can also happen to QKD protocols. However, for a man-in-the-middle attack to work on a QKD protocol the authentication on the classical channel would have to be compromised (just like in a classical version of the attack).

### Unambiguous state discrimination attack

The unambiguous state discrimination (USD) attack [89] is related to the beamsplitter attack described in [90], so we will describe the beamsplitter attack first. Let Eve replace a realistic channel with loss with a perfectly lossless channel and a beam splitter that reflects photons at the same rate they would be lost in the lossy channel. Now, Alice and Bob cannot tell the difference between the lossy and lossless channels. However, when there are multi-photon events, and a portion of the multi-photon signal gets reflected out of the channel to Eve and she holds them in a quantum memory until the bases are announced in the classical phase. Then Eve gets perfect information about the bits she measures after the exchange, which is unacceptable with an epsilon definition of security [59]. In general, beamsplitter attacks are of minimal threat practically as the technology that Eve needs (perfect channel, quantum memory) do not exist yet in the way needed for the attack.

To perform a USD attack, Eve intercepts signals close to Alice and performs an unam-

biguous state discrimination measurement [91] on each one. This measurement will return a correct answer as to the state it measured, or an "uncertain" answer. In the confirmed outcomes Eve prepares a state to send to Bob that she thinks he will measure correctly with the lowest error probability. If the measurement returns "uncertain" then Eve sends the vacuum to Bob and he ideally detects nothing. [89] has a lengthy analysis of the success rates of this attack with different types of states that Eve prepares and sends to Bob.

The best way to counter USD attacks as discussed in [89], is to reduce the mean photon number of the outgoing signals. This will be limited then by the noise floor of your detectors, so care must be taken to characterize all losses/efficiencies in the system and see if the transmission is secure. Dušek et al. have expressions relating all of these parameters to the security criterion.

# Chapter 2

# Feasibility of airborne platforms for QKD

## 2.1 Project motivation

Since the initial publication of protocols for Quantum Key Distribution (QKD), experimental demonstrations have tried to advance the environments and conditions in which QKD can be done successfully. The motivation for this chapter is help determine next steps for advancing the free-space QKD demonstration we have developed. There are many reasons to look at doing QKD to a moving airborne platform. There have been a recent explosion in free space laser communication technology. From light detection and ranging (LIDAR)[92, 93, 94] to faster and more directed classical communication for satellites [95, 96, 97, 98], there is a lot of interest in protocols that can be used with free-space laser communication [99, 100]. Some involve air-to-air, air-to-ground links, or space-to-ground links but the hardware for all of these modalities is often very similar. While our ultimate goal here is to extend the range of QKD by establishing keys with satellites, other airborne platforms can be useful testbeds [101] and actual link distribution options.

QKD as an optical protocol has more strict operating conditions than standard free-space laser communication. These requirements include things like night operation, smaller field of view optical systems, and minimal reflections in the collection optics (as this disrupts the polarization encoding of the bits). There is a lot of infrastructure and interest for airborne and space platforms for laser communication, which QKD can leverage. Because airborne missions are costly in time and resources, it was reasonable to survey the literature to find what aspects of QKD had already been tested on airborne platforms to

help our decision making process for the direction of our experiments. It was found that aircraft and balloons were the most reasonable candidates for airborne QKD tests so this chapter looks at the risks, possible outcomes, and tool development to facilitate testing on each of these platforms.

### 2.1.1 Previous results towards space demonstrations of QKD

Optical channel loss and key rate extrema are being advanced in many different types of QKD protocols and channel modes. Our main interest here is towards space-based QKD, so we are concerned with long distance, free-space experiments. Progress in this category of QKD demonstrations has come a long way in the last 15 years. We will now take a chronological look at those advancements towards space-based QKD.

Earliest demonstrations of free-space QKD links were in 1992 by Bennett et al. [90] in a lab, with a distance between Alice and Bob of 32 cm. The first outdoor link between parties was demonstrated in 1996, with a link of 75 m performed in daylight[102]. The fact it was done in a lit environment is significant as background light can have a detrimental contribution to errors in the detected signal, and most free-space proposals only consider night time key exchanges. Over the next 5 years links were tested over increasing distances on the order of a kilometer [103, 104, 105, 106]. These experiments were done in both light and dark conditions, and with the exception of [107], are basically the last to do so. With the increasing link distances, the loss in the devices needed to be reduced. These additional errors caused by light environments could not be accommodated with increasing link lengths.

The next big jump in demonstrations of link distances made links on the order $\sim 10$ km, the first of which was 23.4 km in 2002 by [108]. The physical link used in this experiment was between two mountain peaks in southern Germany, which represented an atmospheric environment that had not been explored in previous experiments. The next few works build on this step by accomplishing 10 km in daylight [107], using entangled photon sources [109], and key exchanges over long time periods [110]. Building on a large collaboration and equipment set up, in 2007 QKD was demonstrated on what is currently the record free-space distance of 144 km between two of the Canary Islands [111]. Each of these advancements addressed some aspect of QKD that is required for useful space links.

Up to this point, all of the demonstrations of free-space QKD links had been between static endpoints. This was certainly a required first step, but clearly if the goal is to exchange key in some fashion with a moving satellite (even geostationary orbits are not totally static, they are continually correcting their orbit to hold position) we must then look

to demonstrating QKD on moving platforms. The main focus of this chapter is to evaluate different testing modalities for non-static QKD links. To date, balloons, airplanes, and trucks have all been used to provide non-static links for QKD; these will now be discussed in detail.

Nauerth et al. first demonstrated QKD to an aircraft at a range of 20 km at night [112]. The experiment had the transmitter on the moving platform (a Dornier 228 aircraft) and the receiver was mounted on the ground. The aircraft flew in a rough semicircle with an angular speed of $\sim 0.2\,\mathrm{deg}\ /\mathrm{s}$ for $\sim 10$ min, and they measured the link loss to be 38 dB. The quantum link was at 850 nm which was overlapped with a classical data optical channel at 1550 nm. They used a standard BB84 protocol without decoy states added and achieved a quantum bit error rate (QBER) of 4.8%. In a single pass they were able to achieve 80 kbit of key.

This was a significant achievement, however there are a few ways in which it could be improved. First, the key bits sent were not random, so no secure key was extracted from the final detections. While it is possible to predict what the final secure key rate is from parameters estimated in the key exchange [113], secure key was not actually distilled from the detected key bits. Second, beam steering on the plane was done with steering mirrors, which will affect the polarization state of the photons (see subsection 1.2.2). The experimenters got around this by pre-calibrating the state deviation caused by the mirror system. This calibration was not done over temperature ranges, nor in real time. Though they obtain good results, not relying on pre-calibration is a way this experiment could be improved.

Wang et al. were concurrently working on testing a balloon-based moving platform [114]. This experiment also put a transmitter on a floating hot air balloon platform 20 km away, running a decoy state BB84 protocol. They tested the motion tracking on ground based gimbal mounts (40 km), and tested the system with a static, high loss channel on the ground (96 km, 50 dB). Testing with three different environments helps address some of the major remaining obstacles (pointing, channel loss, environment) for a satellite based QKD system. In the post-processing of the key they also fully extract secure key accounting for finite-size effects [115, 116]. They obtained secure key rates of 150 bits/s with QBER of 2.8% for the 2040 km links, and 48 bits/s with QBER of $\sim 4\%$ for the 96 km link.

Both systems discussed so far use weak coherent pulse sources installed on the moving platforms to simulate the space link. It is known that these kind of sources can be secure in a modification of the security proof of BB84 [113], but the original proof assumed a true single-photon source. Zhongkan et al. also demonstrate a moving source on a balloon but use spontaneous parametric down conversion (SPDC) to generate entangled photon

pairs [117]. While they do not actually perform QKD in this work, they achieve a major technological milestone showing a functioning SPDC source that was robust to conditions on a balloon environment at 35.5 km. The source they constructed was not only robust to a rocket launch and operation on a satellite, it survived a failed rocket launch, explosion, and was found still operational with good performance characteristics on a beach a few weeks later [118, 119]. The Ling group also just announced that they had successful photon generation from an entangled source in space [120].

The last moving platform that should be mentioned here is work by our group in Bourgoin et al. [121]. Here we tested a QKD link to the back of a pickup truck $\sim 700$ m away, but with a few significant differences from the aforementioned experiments. In this experiment the receiver was on the moving platform, not the source. This system also had active polarization compensation, and a custom tracking system. The next step for this experiment was to test it on an airborne platform. We then took almost every component and upgraded them to parts that are suitable for space. The development of these components is looked at in chapter 3, but the question of which airborne platform to test with was still an open question.

There are many challenges associated with testing a QKD system involving a moving platform. The most significant are:

- tracking and pointing the sender and receiver apparatuses
- environmental stability of hardware (thermal, pressure, vibration, etc.)
- simulating the representative flight path of target space vehicle (link duration, speed, acceleration, etc.)
- ground station environment and setup timeline
- classical link for live key distillation

We have already seen optical links to aircraft and balloons demonstrations reported in the literature, but in different link configurations. It is very costly in terms of time and finances to prepare for an airborne mission, so it should be carefully considered what platform will provide the most experimental benefit. The flight test platforms that will be considered here are aircraft and balloons (hot-air and stratospheric). Other options could include rockets or drones, but financial or government restrictions prevent easily using these other test platforms. We will now consider the two feasible flight platforms and how they address the testing challenges listed above.

**Contributions**

I did everything in this chapter supported by Thomas Jennewein, the balloon flight data was provided by the Canadian Space Agency's stratospheric balloon program (Stratos) campaign. Field testing in the aircraft was organized by myself, with the assistance of Chris Pugh, Brendon Higgins, and Thomas Jennewein.

## 2.2 Stratospheric balloon platform mission assessment

There are two potential varieties of balloons that could be used to test our airborne payload, hot air balloons and stratospheric (or weather) balloons. Local regulations where this work was carried out lead to hot air balloons not being a viable option. To fly at night we would have to tether the balloon at a distance of at most 200 m, which was about the same distance scale as the ground based truck trials. Therefore we turned our attention to other types of balloons.

Stratospheric balloons are one potential flight testing platform for QKD devices. However, balloon test platforms are very expensive for the amenities we require, and often are one-time use for a particular payload [122]. This means that the test must be worth the risk to the equipment and costs. As there is not a straightforward way to quantify risk, a method was developed specific for this projects' test objectives. There are lots of atmospheric modeling methods [123], but for our quantum channel we are concerned with relatively simple aspects of the transmission. We are not imaging nor does the mode of the single photon significantly affect the measurement outcome. So the modeling we implement here is focused solely on geometry and optical losses of the channel.

These types of balloon platforms have a long heritage of testing space-bound hardware. Stratospheric balloons of the type that the Canadian Space Agency (CSA) and Stratos uses have max altitudes of 12.2 km and carry a gondola that holds multiple payloads to be tested on the flight. Planning such a mission can be very challenging, coordinating up to eight experiments for standard float time of 12-24 hours and managing limited communication and power budgets. For the following assessment we assumed certain amenities provided by a potential option flying with Stratos in the 2015 campaign based out of Timmins, ON. The particular mission offered was utilizing the CARMEN gondola that can rotate and has a platform aboard that can tilt to point payloads within $\sim 5^\circ$ of a target above 25 km (see Figure 2.1).

The other experiments already slated on this mission were interested in daylight and sunrise so the plan was to launch early morning so that they can use sunrise and the day

Figure 2.1: Photo taken of the CARMEN gondola used in the 2014 and 2015 Stratos stratospheric balloon campaigns. It has the ability to rotate and point payloads to a specific target with $\sim 5°$ accuracy.

for most of the mission. This time constraint will impose limitations on how long we can exchange key as the light level from the sun will be higher at altitude than it would be on ground at a given time. Also there is about a two week window in the year at the end of August / beginning of September that the jet stream above Timmins switches from flowing west to flowing east. This time is called the "turnaround" and is when missions are launched to try and minimize how far they can drift while afloat.

The most catastrophic thing that could happen in a stratospheric balloon test of a QKD receiver is hardware destruction by physical mutilation [122]. This would require a completely new prototype to continue testing and development and thus we have to set some sort of goal experiment parameters that we would need to achieve so that the risk of total destruction (to us) would be worth it. The main parameters of qualifying a "successful mission" for a balloon airborne platform are link duration, total number of photons collected from the link, link angular speed, and link distance. Most of these parameters however are dependent on link time, which in turn is a function of the flight path.

For the flight time to be useful, and the fact that it is a subset of the link time, we will quantify risk as categories based on how much link time is usable for experiments. Estimates of the time needed for the pointing process could potentially take as little as a

few minutes, so link times of $\leq 5$ min will constitute a mission failure as that leaves no margin for complications or delays. Link times $\leq 30$ min are high risk as it does not allow for much time for unexpected delays like the gondola starting pointing the wrong way, gondola bouncing, or an intermittent cloud or exhaust trail blocking the channel. Also if the pointing system does not lock on immediately then by the time it does, there could be very little link time left. Link times of $\leq 60$ min are assigned moderate risk. On the whole they could provide some productive experiment time, but again pointing delays and gondola system malfunctions could cut into the link time. Finally, link times of $\geq 60$ min are low risk and should provide good experimental results. See Table 2.1 for a summary.

Table 2.1: Defined risk categories based on the length of the link time possible for a particular experimental flight.

| Link Duration | $<$ 5min | $<$ 30min | $>$ 30min | $>$ 1h |
|---|---|---|---|---|
| Probability of Experimental Success | Fail, or success very unlikely | With high risk | With moderate risk | Low risk |

Since the main reason for testing the payload on a moving platform is to emulate the environment and motion of a satellite, the desired flight path parameters will be drawn from studies of satellite passes [49]. However there is little control often of the flight path of a stratospheric balloon so we look at data from the 2014 Stratos missions launched out of Timmins, ON. We received the last modeled flight path before launch as well as the actual flight path data for all seven missions launched that campaign season. From this we could calculate timelines and possible link times for a QKD experiment on that flight.

Much of the analysis in this section is dependent on the launch location in Timmins, ON. This is primarily due to the fact this was the location that flight opportunities could be found. The launch site moves all over the world, but 2014 and 2015 both happened to be in Timmins. A desert location would have been much better for this experiment but there were no flight opportunities launching out of deserts at the time.

### 2.2.1 Logistics

The logistics for dispatching the transmitter ground team are complex. The ground station is highly mobile but takes quite some time to setup and run diagnostics. The ideal timeline would start around noon the day before launch ($\sim$ 15 hours before launch so the transmitter team can setup in daylight), when a site is selected given the modeled flight data at the time. This selection could use or combine multiple approaches, but it ultimately relies on the team visually inspecting the pre-flight modeled flight paths. Figure 2.2 shows an

example of a flight path forecast in green and where it actually went in purple. Figure 2.3 shows satellite photography of the transmitter area show in Figure 2.2.

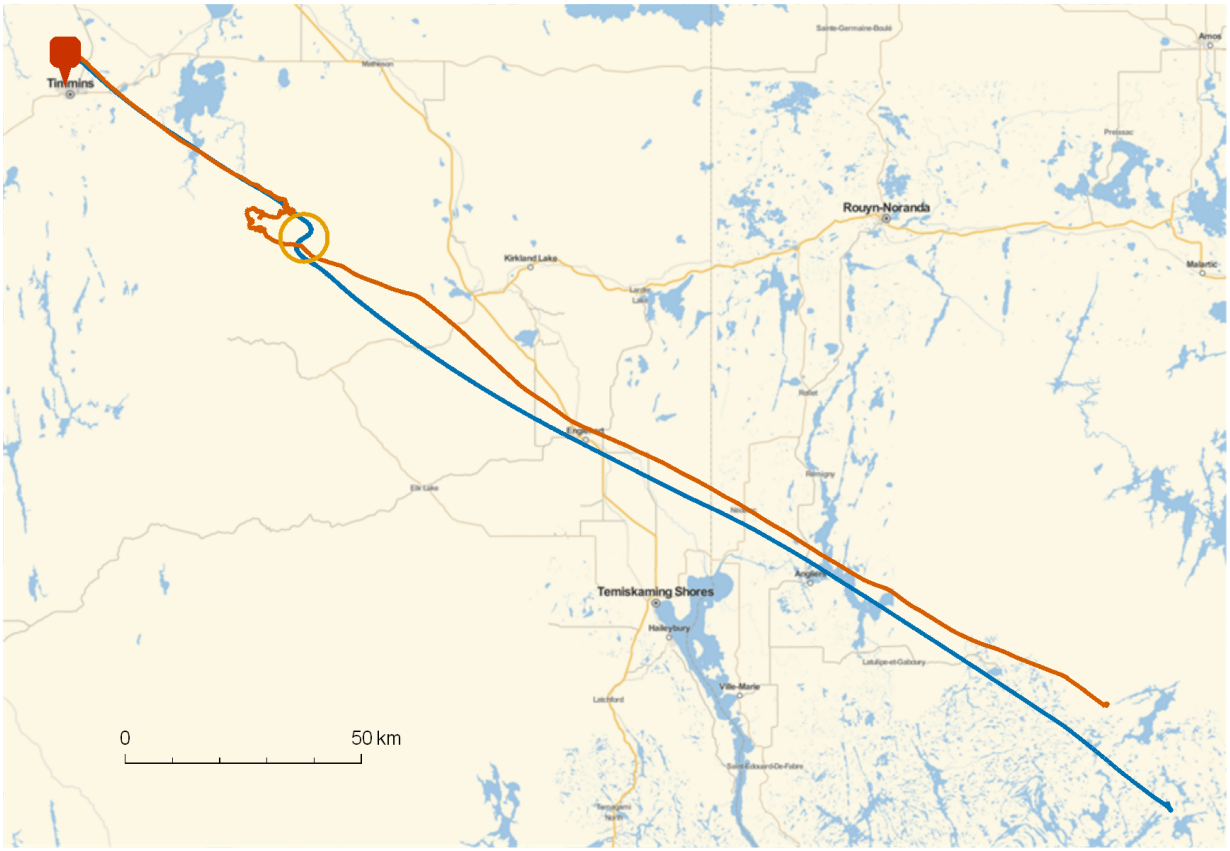



Figure 2.2: Pre-flight modeled trajectory forecasts (blue) and actual flight path (red) for NIMBUS 3. The orange circle represents where the visually selected transmitter was placed as the jog in the path seems to indicate it would spend more time in this area. Source: CSA Stratos Science 2014 Campaign Trajectories Profiles Summary.

Practically, this is not the only factor influencing the site selection. As the launch site is in northern Ontario, much of the terrain is inaccessible or remotely accessible with logging roads. This adds another layer of difficulty to actually getting to the site selected as it could be the case that the nearest road is several kilometers away, and the equipment cannot be carried by hand very far. Additionally, the site (or somewhere nearby) has to have stable parking and footing for the transmitter stand and trailer and a clear view of the sky for the transmitter up to the 45° cone of visibility assumed. This could require

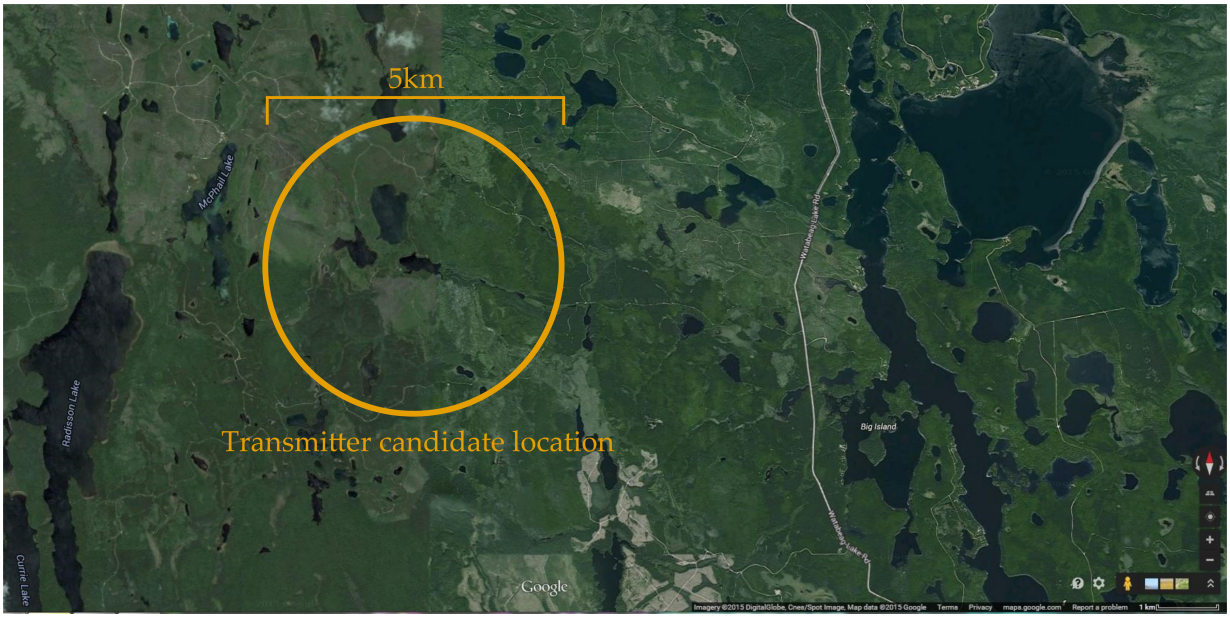



Figure 2.3: Satellite photography of transmitter candidate location from Figure 2.2. Note the lack of roads and heavy foliage. Source: Google Maps.

setting up patio stones and pruning foliage around the site. This could be done in the remaining daylight but then the rest of the set up might have to be done at dusk making it more challenging.

To elaborate on the choice of the size of the cone of visibility from the transmitter, see Figure 2.4. There are 2 major things that contribute to the limit of cone: the hight of the trees and size of the clearing, and the atmospheric losses at a particular angle to float altitude, assumed here to be 30 km. The modeling in Figure 2.4 is derived from [124] and shows the individual contributions to the loss from diffraction, pointing, and turbulence (plus the final 6 dB for the losses in the QKD receiver). It shows that by assuming the QKD system can operate with $\sim$ 45 dB this allows for a link up to about 60 ° from the horizon. However even at 45° the link loss is only about 48 dB. We modeled this before constructing the new devices for the reviver, and the actual channel contributions are below what we have demonstrated with similar hardware. It should also be noted that in [125], demonstrated that finite size Bennett-Brassard 1984 (BB84) can be done above 45 dB, so that combined with improvements in the efficiency of the receiver optics would make 45° field of view reasonable. Any more than 45° could be limited by the local geography, so this is a conservative upper bound on what the visibility the transmitter has of the receiver.

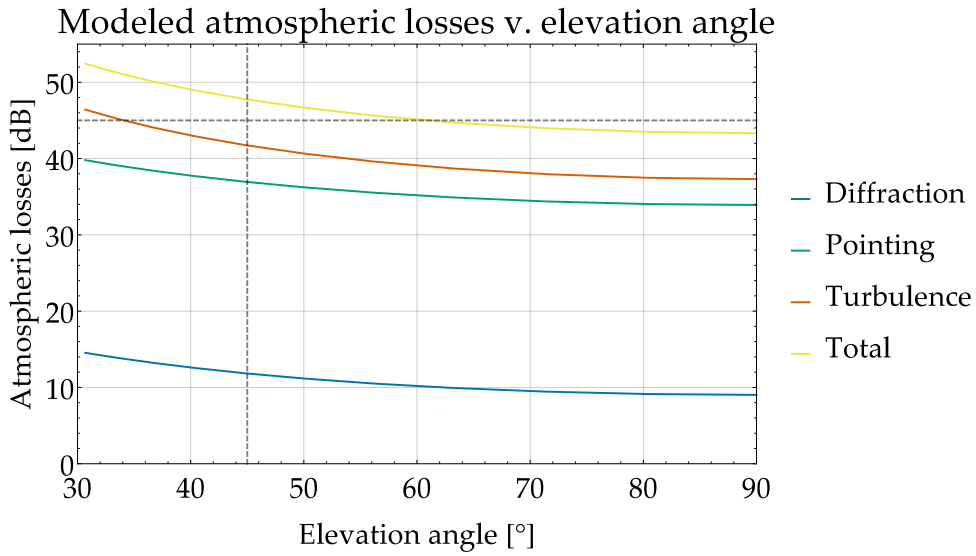



Figure 2.4: Plot of the modeled link loss through the atmosphere to a balloon at 30 km. The transmitter was modeled at rural sea-level location with a transmitter with a diameter of 12 cm. The receiver was modeled to have an aperture of 10.1 cm, and an efficiency of 25% (6 dB). The link was assumed to achieve a pointing accuracy of 0.0033°. The curves are stacked so that they add up the the final total loss curve, which is just all of the previous sources plus the loss in the receiver optics, 6 dB. The dashed lines indicate the 45° cone range and the 45dB loss target we had already demonstrated. We knew the system should be able to handle a few more dB loss and we wanted to maximize our link times but increasing the cone.

Experience has shown that a reasonable estimate of duration for this is minimum 2.5 h, with a team of at least three people. However, unanticipated tasks such as clearing branches and brush may add greatly to this time (or to the personnel required).

### 2.2.2 Experiment timeline

From the past experience of the Institute for Quantum Computing (IQC) team, the latest time this experiment could be successful is about 60 min before sunrise. This combined with the conservative calculation of sunrise being 30 min earlier at the balloon float altitude (40 km) means that in the launch window proposed (early September) the latest that the experiment could run is 04:22.

Table 2.2: Timeline for the experiment setup relative to balloon launch time.

| Time relative to balloon launch | QKD experimental task/event |
|---|---|
| Minus 15 hours | • Selection of initial transmitter area based on best available flight path forecast<br>• Dispatch of team and equipment to initially selected area |
| Minus 12.5 hours | • Arrival at initially selected area<br>• Begin survey to determine final location |
| Minus 10 hours | • Select final location<br>• Prepare the location (i.e. clear vegetation, leveling of ground) |
| Minus 7.5 hours | • Start of transmitter setup |
| Minus 5 hours | • Completion of experimental setup (during daylight)<br>• Start testing of experimental setup |
| Launch of balloon | • Transmitter ready for balloon contact |

The other aspect important about the experimental time window is the travel time to the site selected for the transmitter. Since it will probably be necessary to take a small trailer with a generator and all the set up equipment on logging roads, the speed they can travel is greatly reduced. Also, when the team arrives it will take hours to clear and prepare the site, set up and align the transmitter, and calibrate all of the components to be ready for the balloon's expected overflight. Depending on the location and topology of the setup location, it could be impossible for the transmitter crew to be ready when the balloon arrives. Model volatility is not well characterized here, but of course the closer to launch the better the models for the flight become. So, the transmitter team would need to wait until the last possible moment to leave for the expected optimal transmitter location.

After the transmitter is operational and it is possible to address the balloon, there will be some additional time needed to lock the pointing and tracking on both sides (ground and balloon) of the experiment. The timeline for the experiment setup relative to the balloon launch time is summarized in Table 2.2.

### 2.2.3 Transmitter location options

Attempting to establish the QKD link during the balloon's initial ascent from Timmins airport was originally proposed as a good way to mitigate risk and reduce pointing losses. However, the pointing system of the payload gondola only activates above 25 km. This is because after liftoff the gondola sways and bounces and this is the altitude by which this motion is mostly damped. It is highly unlikely that the balloon is still within the range of the transmitter when it achieves this altitude. We propose three alternative options for the location of the transmitter, which were implemented using Mathematica and the provided data from historical missions:

- **Option 1** Locate the transmitter in Timmins, close to the airport, but not directly so as to avoid local light pollution.
- **Option 2** Select a location from the pre-flight forecasted balloon trajectory where the optimal place for the transmitter would likely be. This is most representative of the actual process to decide on a transmitter location, as this would be based on the information available just before the hypothetical launch.
- **Option 3** Estimate (again from pre-flight forecasted trajectory data) where the balloon will be above the 25 km altitude, at which point the gondola pointing systems can be engaged. Then a location would be chosen to maximize the expected time available to address the balloon payload, with the added constraint of launching just before dawn.

Figure 2.5 shows a sample of the locations considered for a particular historical flight dataset. Here the plot is in degrees latitude and longitude from Timmins and the transmitter has a field of view of 45°. This value is approximate, based on projected optical losses to the payload such that the edge of the cone is where the losses become unacceptably high. Figure 2.6 has the selected transmitter locations and field of view cones for all seven missions.

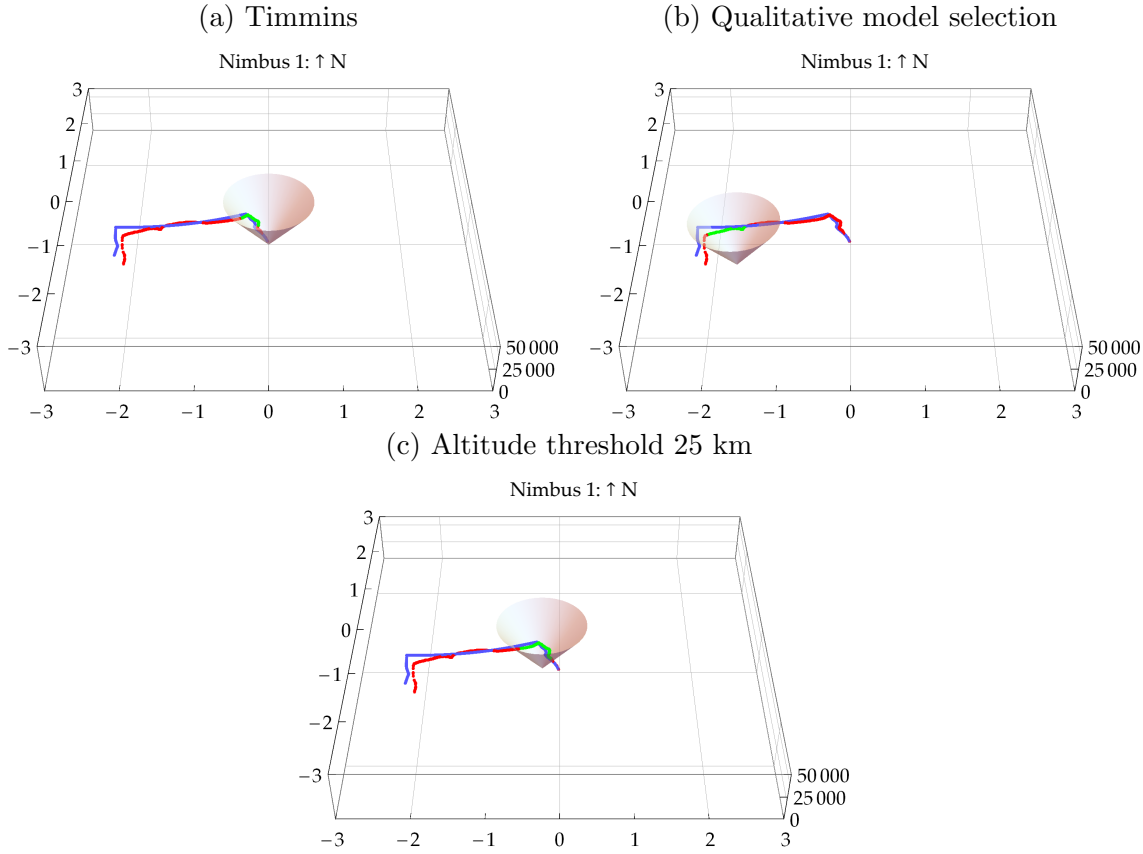



Figure 2.5: Three different options for selecting the transmitter location give pre-flight modeled trajectory forecasts. The cone represents the field of view of the transmitter at a particular location, currently set to be 45° from normal to the ground. Blue is the modeled path, red the actual path the balloon took, and green is the part of the actual path that could be viable for the QKD experiment.

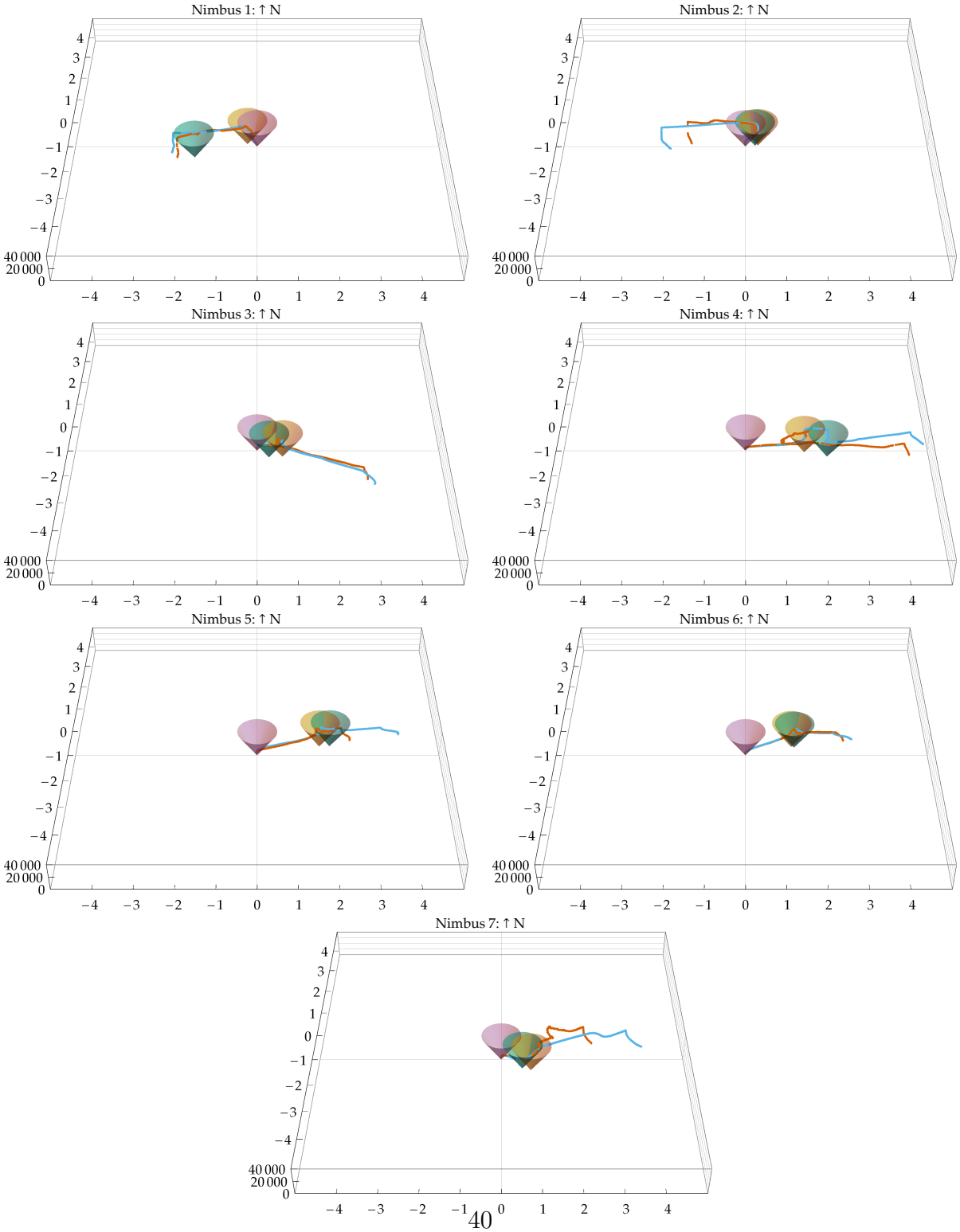



Figure 2.6: Plots of all of the simulated transmitter locations for each mission, pink being at Timmins, green visually selected, and orange altitude threshold. Blue tracks are the provided modeled path before launch and red the actual path for that mission.

The current proposal for the 2015 Stratos CARMEN flight is to launch at 03:00. The seven historical Stratos flights from the 2014 campaign have been analyzed for the time when they reached pointing altitude (25 km) to 1.5 h before sunrise for the amount of feasible experiment time that would be available. The timelines for the launches are calculated from the respective historical flight data where the latest the experiment could run is 04:22. Other assumptions are that the transmitter has a 45° field of view and that the launch starts at 02:00, as 03:00 would be too late. Also, per discussions in teleconferences with the CSA, it is likely that flights 3-7 are more representative of this proposed flight (after turnaround) so that success in the first two flights is less important.

The terms used in the discussion for following section are as follows:

- **Delay to connection** The time from when the balloon is launched to the time when the balloon is in view of the transmitter location
- **Connection duration** How long the balloon is in the optical field-of-view (FOV) of the transmitter location
- **Usable experiment time** Amount of connection duration when the balloon is above 25 km in altitude, allowing active pointing

### Option 1: Transmitter Located at Launch Site (Timmins)

Suppose the transmitter is placed at Timmins (11 min drive from the airport) and the flight starts at 02:00. Table 2.3 shows the simulated mission parameters from the seven flights in 2014. Hypothetically, in flights 2 and 3 there is more than 5 min of connection time which would be sufficient for data collection, however, this would assume that pointing was already established. This placement option is infeasible for flights that would resemble the current campaign.

### Option 2: Transmitter Location Based on Predicted Flight Path

If the transmitter were to be placed by selecting a location based on the pre-flight modeled balloon trajectory, we could potentially get up to an hour of connection duration (see Table 2.4). As shown in Table 2.5 for the usable flights, it will not be possible to dispatch the transmitter team right at launch. They would have to be dispatched some time earlier (ideally 15 hours), with the potential location based on older flight trajectory forecasts.

Table 2.3: Flight parameters given a transmitter location approximately 11 min drive time away from Timmins airport. N/A represents no connection made for those flight with a transmitter in Timmins. The launch was simulated at 02:00, and sunrise at max altitude is 04:22.

| | | Nimbus 1 | Nimbus 2 | Nimbus 3 | Nimbus 4 | Nimbus 5 | Nimbus 6 | Nimbus 7 |
|---|---|---|---|---|---|---|---|---|
| Transmitter location | Lat (N) | 48.49 | 48.49 | 48.49 | N/A | N/A | N/A | 48.49 |
| | Lon (W) | -81.35 | -81.35 | -81.35 | | | | -81.35 |
| Delay to connection [min] | | 291.4 | 133.7 | 51.5 | N/A | N/A | N/A | 18.0 |
| Connection start time | | 06:51 | 04:13 | 02:51 | N/A | N/A | N/A | 02:18 |
| Connection end time | | 08:03 | 06:50 | 02:59 | N/A | N/A | N/A | 02:18 |
| Connection duration [min] | | 72.5 | 156.3 | 7.5 | N/A | N/A | N/A | 0.5 |
| Usable experiment time [min] | | 0 | 8.3 | 7.5 | N/A | N/A | N/A | 0.5 |

Table 2.4: Flight parameters given a manually selected transmitter location from the modeled data.

| | | Nimbus 1 | Nimbus 2 | Nimbus 3 | Nimbus 4 | Nimbus 5 | Nimbus 6 | Nimbus 7 |
|---|---|---|---|---|---|---|---|---|
| Transmitter location | Lat (N) | 48.3911 | 48.5558 | 48.2061 | 48.5194 | 48.8542 | 48.8658 | 48.8619 |
| | Lon (W) | -82.2800 | -81.1803 | -80.6719 | -79.5069 | -79.3417 | -80.0003 | -79.9894 |
| Delay to connection [min] | | 374.4 | 75.7 | 78.5 | 93.0 | 103.5 | 302.6 | 488.5 |
| Connection start time | | 08:14 | 03:15 | 03:18 | 03:33 | 03:43 | 07:02 | 10:08 |
| Connection end time | | 10:17 | 06:31 | 06:43 | 15:31 | 09:32 | 09:29 | 15:54 |
| Connection duration [min] | | 123.0 | 196.0 | 205.0 | 718.9 | 349.0 | 146.6 | 346.0 |
| Usable experiment time [min] | | 0 | 66.3 | 63.5 | 49.0 | 38.5 | 0 | 0 |

### Option 3: Transmitter Located at Trajectory Operational Altitude

If the transmitter were to be placed by selecting a location based on where the predicted balloon trajectory reaches its expected operational altitude, we could potentially achieve up to a half hour of connection time. The other connections are not really long enough to be useful due to pointing acquisition time. This placement algorithm works with high risk on 3 of 5 historical flights that resemble the current campaign. As shown in Table 2.6, for the usable flights there it would not be possible to wait until the time of launch to dispatch the transmitter team. They would be sent some time earlier with the potential transmitter location based on older trajectory projections (Table 2.7).

Table 2.5: Driving times (min) from launch site to the projected transmitter location (from Google Maps directions to the locations chosen) determine the latest possible decision point of the ground station location. Ideally, the transmitter location will be chosen on the day before launch (15 h in advance) so that the experimental setup can be done in daylight which should take about 2.5 h. No times are listed for flights 1, 6, and 7 because there was no usable experiment time.

| Nimbus flight # | 2 | 3 | 4 | 5 |
|---|---|---|---|---|
| Time from launch to connection [min] | 76 | 79 | 93 | 104 |
| Drive time to location + setup [min] | 188 | 279 | 269 | 338 |
| Distance to location [km] | 28 | 134 | 158 | 231 |
| Latest transmitter deployment [min] | 112 | 200 | 176 | 234 |

Table 2.6: Flight parameters given a transmitter location with the objective of maximizing connection time once the balloon reaches 25 km, to ensure the availability of gondola pointing.

| | | Nimbus 1 | Nimbus 2 | Nimbus 3 | Nimbus 4 | Nimbus 5 | Nimbus 6 | Nimbus 7 |
|---|---|---|---|---|---|---|---|---|
| Transmitter location | Lat (N) | 48.5897 | 48.5358 | 48.2353 | 48.4236 | 48.8695 | 48.8497 | 48.0458 |
| | Lon (W) | -81.6153 | -81.0122 | -80.6628 | -79.7414 | -79.6319 | -80.0864 | -80.5447 |
| Delay to connection [min] | | 272.4 | 87.7 | 77.5 | 68.5 | 71.5 | 297.9 | 55.0 |
| Connection start | | 06:32 | 03:27 | 03:17 | 03:08 | 03:11 | 06:57 | 02:55 |
| Connection end time | | 08:26 | 06:09 | 06:40 | 15:32 | 08:59 | 09:18 | 06:12 |
| Connection duration [min] | | 114.0 | 162.0 | 203.0 | 744.4 | 348.5 | 140.7 | 197.5 |
| Usable experiment time [min] | | 0 | 54.3 | 64.5 | 73.5 | 70.5 | 0 | 87.0 |

Table 2.7: Driving times (min) from launch site to the projected transmitter location (from Google Maps directions to the locations chosen) determine the latest possible decision point of the ground station location. Locations 1 and 6 are not listed as there was no usable experiment time.

| Nimbus flight # | 2 | 3 | 4 | 5 | 7 |
|---|---|---|---|---|---|
| Time from launch to connection [min] | 88 | 78 | 69 | 72 | 55 |
| Drive time to location + setup [min] | 185 | 260 | 271 | 355 | 298 |
| Distance to location [km] | 32 | 124 | 152 | 249 | 181 |
| Latest transmitter deployment [min] | 97 | 182 | 202 | 283 | 243 |

### 2.2.4 Conclusion

The results from the above modeling of a 02:00 launch are shown in Table 2.8, and are summarized below:

- **Option 1**: locating the transmitter at the balloon launch site is infeasible.
- **Option 2**: choosing the expected optimal transmitter location based on the predicted balloon flight path worked with moderate risk in 3 of 5 historical missions similar to the proposed flight. This option does have the problem that the transmitter team must be deployed to the selected location hours before the launch (ideally more than 15 hours) to a site based on less accurate modeled flight path data.
- **Option 3**: optimizing the time after the balloon reaches the pointing altitude, we observed moderate or low risk links for 5 of the 7 historical missions. This option does have the problem that the transmitter team must be deployed to the selected location hours before the launch (ideally more than 15 hours) to a site based on less accurate modeled flight path data. A launch time of 02:00 therefore presents a moderate risk to the mission but still could be considered. Launching at 01:00 or earlier could linearly increase the usable time, potentially making a successful QKD link more feasible.

Out of five representative historical flight profiles from the Stratos 2014 campaign, Options 2 and 3 would only have been viable for three flights (see Table 2.8). For any reasonable probability of mission success, 02:00 would be the latest acceptable balloon launch time. While moving the launch time earlier would increase the potential duration of optical links, the challenge of pre-positioning the transmitters without definitive knowledge of the balloon flight trajectory remains. It is therefore concluded that a stratospheric balloon is a suitable platform for QKD experiments, but under the launch conditions currently available is not feasible.

## 2.3 Aircraft feasibility analysis and simulation

Helicopters or fixed-wing aircraft would resolve the main challenges associated with a stratospheric balloon given the balloon has a non-deterministic flight path. There would be a high probability of achieving the secure key exchange science objectives due to the ability to control the aircraft flight path in order to be within range of the ground-based

Table 2.8: Summary of the three transmitter location selection algorithm results for all the 2014 Stratos campaign. The delay to connection describes how long into the balloon flight visual contact is made with the transmitter, and the usable experiment time ensures that pointing of the gondola is possible for the experiment (i.e. the balloon is above 25 km).

| TL Location | Launch site | | Visually predicted | | Operational altitude ($l \leq 25$ km) | |
|---|---|---|---|---|---|---|
| Mission | Delay to connection [min] | Usable experiment time [min] | Delay to connection [min] | Usable experiment time [min] | Delay to connection [min] | Usable experiment time [min] |
| Nimbus 1 | 291.4 | 0.0 | 374.4 | 0.0 | 272.4 | 0.0 |
| Nimbus 2 | 133.7 | 8.3 | 75.7 | 66.3 | 87.7 | 54.3 |
| Nimbus 3 | 51.5 | 7.5 | 78.5 | 63.5 | 77.5 | 64.5 |
| Nimbus 4 | 0.0 | 0.0 | 93.0 | 49.0 | 68.5 | 73.5 |
| Nimbus 5 | 0.0 | 0.0 | 103.5 | 38.5 | 71.5 | 70.5 |
| Nimbus 6 | 0.0 | 0.0 | 302.6 | 0.0 | 297.9 | 0.0 |
| Nimbus 7 | 18.0 | 0.5 | 488.5 | 0.0 | 55.0 | 87.0 |

| Link Duration | $< 5$ min | $< 30$ min | $> 30$ min | $> 1$ h |
|---|---|---|---|---|
| Probability of Experimental Success | Fail, or success very unlikely | With high risk | With moderate risk | Low risk |

transmitters. The relative speed between the ground transmitter and the airborne receiver would also be representative of a satellite pass. Depending on the aircraft, a researcher may accompany the payload in the cabin and have direct access to resolve any issues. Finally, the payload should be recovered intact after the flight.

The non-deterministic flight path of the stratospheric balloon option required extensive analysis to evaluate the viability of the platform for QKD. Additionally, the fact that the payload could be potentially unrecoverable added to the inherent risk of a balloon mission. Aircraft, on the other hand, have deterministic motion and the payload is completely recoverable after testing. Much of the risk with the balloons is associated with the flight path and the ability to position a ground station in a usable location. Planes have more freedom in these respects, so this biggest risk factor is eliminated. There are no constraints on the ground station with an aircraft, provided it has a clear view of the vehicle and the flight path it will take.

In order to assess the feasibility of aircraft for QKD, we must again quantify the risks involved. To begin, we looked at various $2 - 6$ passenger prop planes, as well as larger research planes. The primary criteria we identified were the following (which were not considered in the balloon platform as they were handled by the experienced launch crew):

- Power constraints
- Internal mounting and motion restrictions
- Classical communication link

The power constraint is highly dependent on the vehicle considered, but the consistent solution was simple: bring our own batteries. From the equipment that we had already assembled and is detailed in chapter 3, we estimated our power consumption to be $\sim$ 200Wh. We found commercially available lithium-ion battery packs from [126] that would provide power for a few hours of testing with startup margins and came in sealed cases suitable for rugged conditions. However, they have a finite lifetime as it is well know the slight pressure changes in planes with sealed lithium cells can be catastrophic if the cells fail [127].

The latter two constraints will be addressed in the following sections.

### 2.3.1 Modeling geometric constraints on receiver pointing

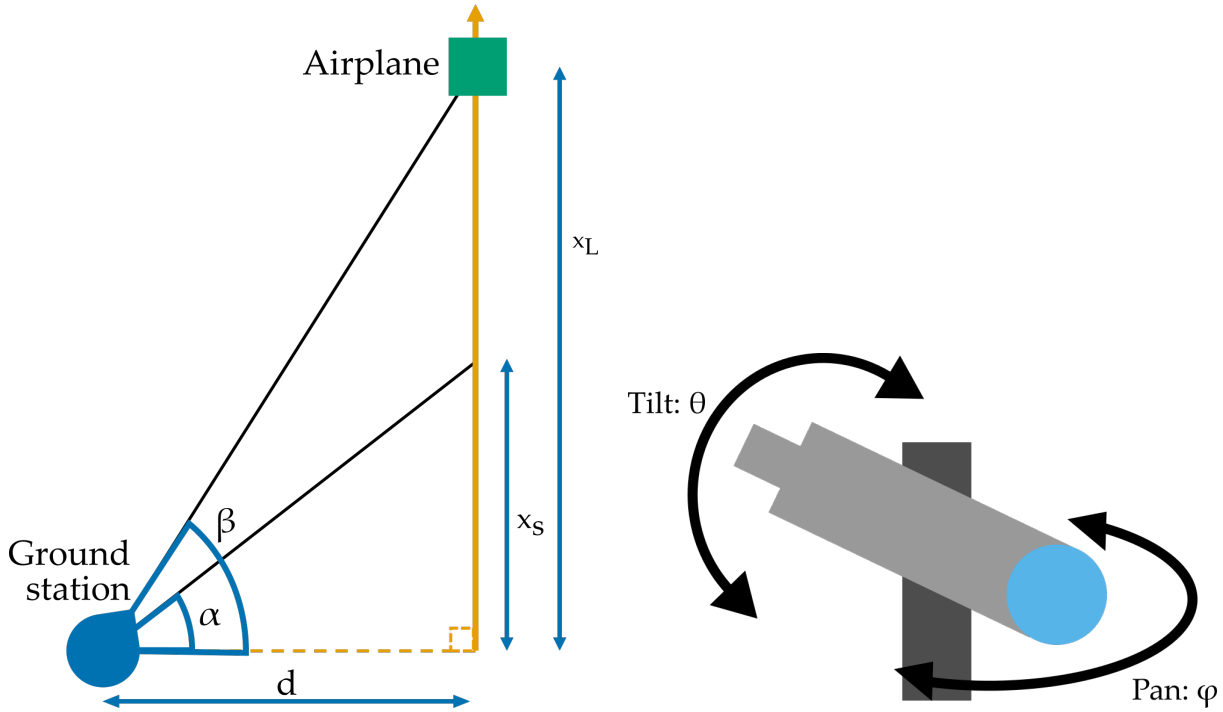
The receiver optics that are mounted in the aircraft are approximately 1.5 m long, which proves to be a problem in most smaller prop planes considered here (see Figure 2.7b). The optics cannot be mounted outside the aircraft because of the drag and turbulence. More importantly, it is difficult to re-certify an aircraft as flight worthy that has had any permanent modification to the structure inside or out [128]. Our solution to mounting the payload must utilize existing infrastructure in the plane, and open windows or doors for lines of sight. For the purposes of this section we will look at a particular aircraft that was used for testing of payload components, Beechcraft Bonanza (Figure 2.7a).

(a) Photo of the Beechcraft Bonanza V-tail that was used for testing and modeling in this chapter. Fun fact: this model is known as the "Doctor-killer" as the tail makes control of the ailerons and the rudder coupled and difficult for beginner pilots. Thanks to Jeff Kehoe for piloting for these tests.

(b) Photo of the installation of the receiver unit in a Beechcraft Bonanza. It can be seen clearly that there is a restricted range of motion within the plane.

Figure 2.7: Beechcraft Bonanza used for modeling in this chapter.

The internal and aperture constraints mean that we need to be able to calculate what is the flight path that will optimize the achievable link time. We will do this with a simple geometric model which uses straight overhead fly-overs, as this is representative of a satellite pass (see [49]).




(a) Labeled distances used to model the flight path geometry for constrained receiver pointing. All distances are in m and angles in radians.

(b) For the reciever mounted in the aircraft, the pan and tilt angles are defined as above.

The modeling tool presented here relies on two sets of parameters: performance parameters of the aircraft, and the angular constraints of the receiver payload. The former can easily be obtained from the vehicle specifications and recommendations of the pilot, and the latter is easily measured by testing the receiver payload on the ground. This safe range of movement will be characterized by two angles, $\alpha$ for the horizontal start of the link and $\beta$ for the end horizontal link Figure 2.8a. We also measure the vertical angular range of the payload, from 0 being level with the floor of the plane, positive angles are pointing up from the floor and negative angles at the floor. In order to communicate with a ground based transmitter, our receiver should never be pointed at angles $\geq 0$. Therefore this range of only negative values will be labeled $\delta$ at the higher end and $\epsilon$ at the lower (more towards the ground) end.

If we assume the plane is flying in a straight, level path some displacement $d$ from the ground station then we can calculate quantities $x_L$ and $x_S$ as follows (see Figure 2.8a for a top down view of the flight path). The flight path will be parameterized by $x$ which is the

position along the flight path measured from the point of closest approach to the ground station. Let $\tau$ be the length of time that a link could be established with the plane flying at a constant speed $v$.

$$x_L = d \tan \beta \tag{2.1}$$

$$x_S = d \tan \alpha \tag{2.2}$$

$$\tau = \frac{x_L - x_S}{v} \tag{2.3}$$

Now we can calculate the link length as a function of $d, x$ and $h$ which represents the height above the ground that the plane is flying at with simple Pythagorean rule. Assume all distances are in meters and angles are in radians for the following calculations.

$$\text{linkLength}[d, x, h] = \sqrt{d^2 + h^2 + x^2} \tag{2.4}$$

The vertical tilt angle of the payload is also dependent on the position of the plane as well and can be expressed:

$$\text{tiltAngle}[d, x, h] = \arctan\left[\frac{h}{\sqrt{d^2 + x^2}}\right] \tag{2.5}$$

Now, since what we are most concerned with out of this model is what will be the flight path that provides the maximum amount of link time, let's parameterize $x$ as a function of $t$. Let $\tau$ be the length of time that a link could be established with the plane flying at a constant speed $v$.

$$x[t, \tau, d] = d \tan(\alpha) + \frac{d \cdot t \cdot \tan(\beta)}{\tau} \tag{2.6}$$

We can also then write the link length, the current horizontal pan angle $\phi$, and vertical tilt angle $\theta$ as a function of $t$.

$$\text{linkLength}[t, \tau, d, h] = \sqrt{d^2 + h^2 + x[t, \tau, d]^2} \tag{2.7}$$

$$\phi[t, \tau, d] = \arctan\left[\frac{x[t, \tau, d]}{d}\right] \tag{2.8}$$

$$\theta[t, \tau, d, h] = \arcsin\left[\frac{h}{\text{linkLength}[t, \tau, d, h]}\right] \tag{2.9}$$

The other important quantity that we are interested in is the angular speed of the payload as a function of time, and specifically the maximum angular velocity of the flight. We can take the derivatives of $\phi$ and $\theta$, solve for the maximum angular velocity which will identify at most 2 possibilities. By inspection the time when $\phi$ is maximized is 0 as the derivative of arctan is $\frac{1}{1+x^2}$. Thus the derivative is maximized when $x$ (or $t$) is minimized. It turns out that both expressions for the maximum angular velocity are independent of $t$, and once given the angular constraints $\alpha, \beta, \gamma$ and $\delta$ the expression for the max angular velocity of the pass can be calculated.

The model given above was implemented with an interactive graphical user interface for use in planing test flights in the field. Given a set of physical angular constraints of the receiver, speed range of the plane, flying height of the plane, and optional plane bank angles, to compute the optimal displacement $d$ of the path from the transmitter. It also provides other flight parameters such as total link time, maximum link length, altitude and Global Positioning System (GPS) information for the vehicle to follow to achieve the modeled path (given a ground station location). See Figure 2.9 for a screenshot of the program and Appendix A for the source.

### 2.3.2 Testing communication systems for airborne platforms

As can be the case, the simpler a task is the harder it is. We have addressed the power and pointing constraint issues for the aircraft test platform option, so all that remains is a classical communication link. This is a commercially solved problem in many ways, but as always there are constraints. One obvious option is to use the cellular network to link the two. The candidate locations that we have for our ground station are located in remote, rural areas which means that there is insufficient cell coverage, and furthermore the antennas are designed for ground level coverage. An aircraft at 1.52 km may potentially not have any service even if it is directly above areas of ground coverage. We did some preliminary testing of these devices in a small private plane and weak and periodic reception, if any in the areas we had identified for ground stations.

Another straightforward option is directed local radio channel, at standard wireless local area network (WiFi) frequencies. We installed an antenna in the Beechcraft Bonanza and did some test flights near the airport in Brampton, ON. Figure 2.10 shows the paths flown where with the limited antenna range of the plane we were able to establish a link and stream GPS data both ways. Figure 2.11 shows the link distance between the plane and the ground as well as the temporal length of the link. Poor weather conditions prevented us from performing more extensive tests. However, we were able to determine that if the

WiFi antenna were pointed co-linearly with the mean direction of the receiver unit then we should be able to obtain a reliable classical link to stream GPS data as well as QKD data for live key distillation.

### 2.3.3 Results

The main outcome of the aircraft modeling was a tool that can take the measured constraints from the aircraft and candidate ground station locations and provide GPS coordinates for a pilot to fly exactly the course needed to maximize the link time. Additionally, Table 2.9 was developed to help facilitate discussions with flight operators. Discussions of experiments that involve shining lasers out of and at aircraft are met with an understandable skepticism in the aviation community.

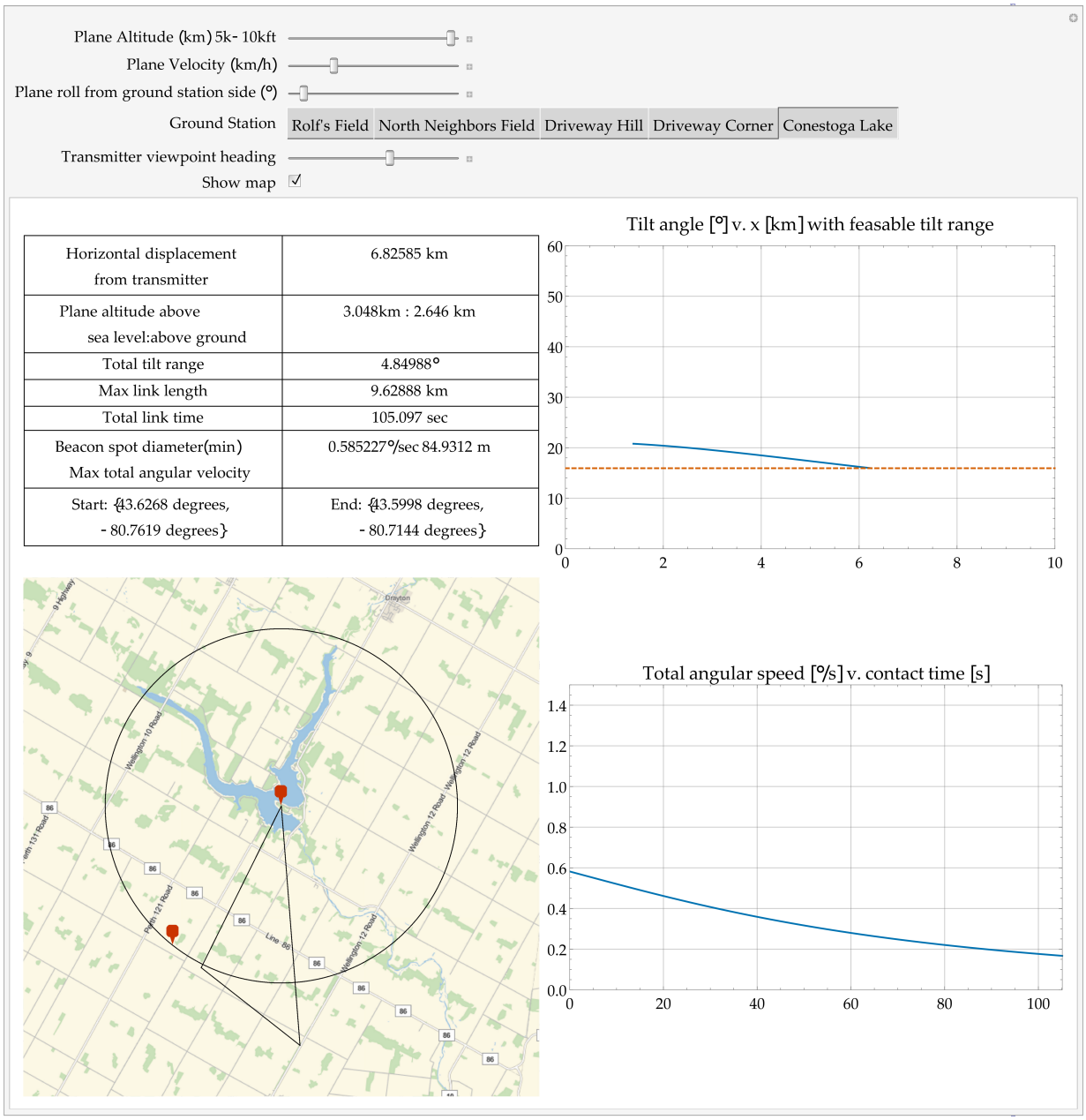



Figure 2.9: Screenshot from the graphical user interface tool to calculate optimal test flights for a QKD mission, as well as explore possible variations.

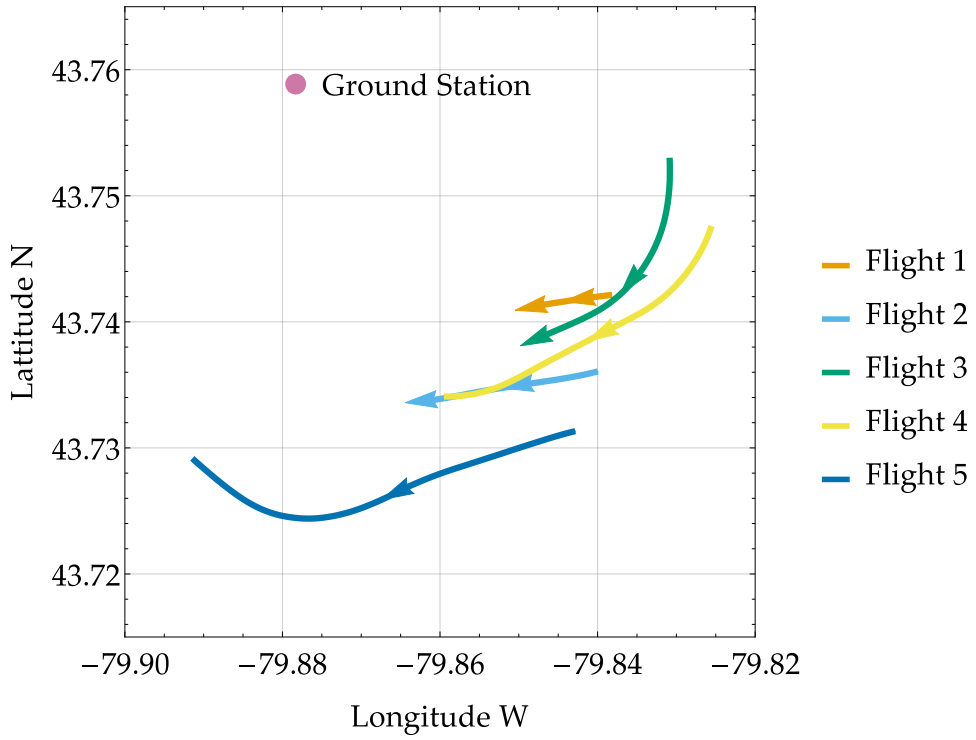



Figure 2.10: Flight paths that were tested to evaluate the classical communication link fidelity. The pink circle was the location of the ground station, and the coordinates are in lat, long. The test flights were circular as this was easier to do in the poor weather conditions.

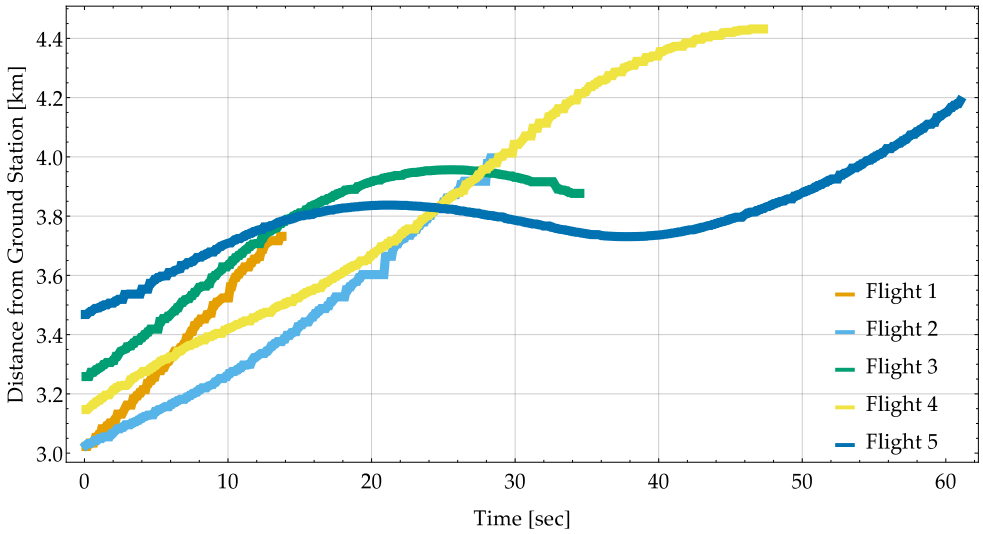



Figure 2.11: Flight paths that were tested to evaluate the WiFi link fidelity. Here the link distances and durations can be seen for each of the five recorded passes. Though the overall link distances and times are short of the desired link times for a QKD path, it is promising that the WiFi system could work.

Table 2.9: Table (part 1 of 2) of derived requirements from aircraft modeling results. Developed to efficiently communicate with parties that can offer airborne platforms for testing our payload.

| ID | Title | Requirement | Comments |
|---|---|---|---|
| FP-010 | Flight weather | A planned flight must only proceeded when there are no clouds between the ground and the vehicle and the winds are calm. | |
| FP-020 | Experiment time window | The flight platform must maximize optical link to times between 1h after sunset and 1h before sunrise. | Actual times depend on the time of the year. |
| FP-030 | Experimental link time per pass | The optical payload in the platform must have at least 100s of contact time per pass over the ground station. | This contact time would mean that we should be able to fit many attempted passes in a single flight. This is representative of satellite passes that have been considered for the QEYSSAT mission. |
| FP-G-030 | Experimental link time per pass | The optical payload in the platform should have at least 300s of contact time per pass over the ground station. | This would make collecting statistics about the transmissions much better and we would be able to extract more key in a single pass. |
| FP-040 | Platform flight speed | The flight platform must fly at a speed that maximizes the optical contact time | This is highly dependent on the interior geometry of the payload and the directions that the telescope can look out of the vehicle. Typically this is as slow as the vehicle can go to maximize the contact time ∼100kts or less. More payload room and field of view means that the vehicle can fly faster if needed. |
| FP-050 | Platform angular speed | The platform must be moving at a peak angular velocity relative to the ground station of at least 0.7/sec. | This is representative of satellite passes that have been considered for the QEYSSAT mission. |
| FP-G-050 | Platform angular speed | The platform should be able to move at a peak angular velocity relative to the ground station of at least 1.2/sec. | This is representative of satellite passes that have been considered for the QEYSSAT mission. |
| FP-060 | Flight altitude | The flight platform must fly at a height that maximizes the optical contact time | This is highly dependent on the interior geometry of the payload and the directions that the telescope can look out of the vehicle. Typically this is as high as possible ∼10,000ft to make the angular speed of the platform the required value. More payload room and field of view means that the vehicle can fly over a wider range of altitudes. |
| FP-070 | Flight path geometry of individual passes | The flight platform must be able to fly in a straight line path above, but offset from the ground station. | The optical links we would like to target are anywhere from 3-10km from the plane to the ground station. This is representative of a satellite pass in a LEO orbit. |
| FP-G-070 | Flight path geometry of individual passes | The flight platform should be able to fly in a circular path around the ground station. | This is to reduce the strain on the pointing motors and aid in debugging problems mid-experiment. |
| FP-080 | Platform variance | The flight platform must be able to fly with the ability to stabilize its course, tilt, pitch and roll variance during active optical link to less than ∼1/s. | Based on the performance of the motors and fine pointing system. |
| FP-090 | Ground station location | The flight activities must be conducted in an area where the surrounding light pollution is minimal over an area of ∼50m radius around the ground station. | Eg. A rural area where the ground has good sky visibility and there is no radio/Wi-Fi signals that will interfere with the classical communication link between the ground and the platform. Can be located anywhere as long as we can transport the ground station equipment there. Our current planned location is in Maryhill, ON. Preliminary analysis suggests suitable locations exist in and around Ottawa. |
| FP-100 | Mass | The flight platform must be able to support the total equipment mass of 100kg (220lb) and at least one personnel to operate the equipment. | Mass Includes telescope and attached optics, coarse pointing motor, driving electronics, classical radio link equipment, and battery power for the equipment. Weight can be reduced if power is provided by the vehicle. |
| FP-110 | Volume | The flight platform payload area must accommodate: a 1.5lx1.2wx1h (m) optical payload and 0.75mˆ3 electronics payload that can be located up to 3m away from the optical payload, 0.5mˆ3 of battery packs can be located up to 3m away from the electronics, and an IQC payload operator in a seat with a laptop. | This volume allows for restricted but useable range of motion of the optical payload if the telescope has a view out of the plane throughout the whole range. |
| FP-G-110 | Volume | The flight platform payload area should accommodate: a 1.5mˆ3 optical payload and 0.75mˆ3 electronics payload that can be located up to 3m away from the optical payload, 0.5mˆ3 of battery packs can be located up to 3m away from the electronics, and an IQC payload operator in a seat with a laptop. | This volume allows for full, free rotation of the optical payload. |
| FP-G-120 | Power | The flight platform should provide 28V unregulated, 200W peak, 100W idle power for the duration of the flight. | Includes a 50W margin for other incidental needs like optical heating or control computer charging. If no power is provided, 2 lithium battery packs will be used. |

Table 2.10: Table (part 2 of 2) of derived requirements from aircraft modeling results. Developed to efficiently communicate with parties that can offer airborne platforms for testing our payload.

| ID | Title | Requirement | Comments |
|---|---|---|---|
| FP-130 | Vibration environment | The flight platform mounting solution must minimize the vibrations the optical payload experiences. | There is no required threshold to damp the vibrations to, we only know that it survives well the vibration environment on a truck. |
| FP-140 | Thermal environment | The flight platform must maintain an internal temperature of greater than or equal to -20C. | Almost all of our commercial components are traceable to being tested in this range. System was designed for stratospheric balloon flights. |
| FP-150 | Optical window | The flight platform aperture where the optical payload is to point out must be empty or made of a material that is not disruptive to polarization and transparent to 785nm and 850nm. | All lasers adhere to safety requirements (see IQC technote). |
| FP-160 | Classical Communication link frequency | The platform must be able to accommodate the 2.4GHz and 5GHz radio antenna in a window to establish a classical network link with the ground station. | |
| FP-170 | Classical communication link antenna | The flight platform must accommodate the placement of a gps antenna in a window inside the vehicle so the primary gps system for the payload has signal. | |
| FP-G-170 | Classical Communication link | The platform should have some built in radio or similar communication capabilities that can be connected to the payload and a receiver on the ground to communicate position data and support live key distillation. | |
| FP-G-180 | Payload Navigational Data | The flight platform should be able to provide a live GPS data stream of the platform position to the payload. | |
| FP-G-180 | Platform Navigational Data Broadcast | The platform should have some built in GPS broadcasting (ADS-B or similar) that the ground station can use to track the vehicle better. | |
| FP-190 | Payload operator | The IQC payload operator must have a network (Ethernet) connection to the payload in flight, and a laptop with them to monitor the payload. | |
| FP-G-190 | Payload operator | The IQC payload operator should have access to the electronics crate and other hardware in flight as well as a network connection to a laptop. | This is to support in flight debugging. |

# Chapter 3

# Component development for satellite QKD

## 3.1 Introduction

Performing demonstrations of long-distance Quantum Key Distribution (QKD) links requires very different devices than those used in lab demos. They often start as lab grade components and are then modified to survive outdoor conditions (vibration, humidity, temperature, etc.). Sometimes to meet these conditions they need to be redesigned from the ground up. We have developed a few key components for long-distance outdoor QKD, which will be outlined in this chapter. Figure 3.1 shows a schematic of how some of these pieces fit together.

The first component that will be discussed in this chapter is a small, low-power, single photon detector package. The device has four independent detector channels and performance characteristics competitive with lab grade devices, while meeting many requirements for operation in more rugged environments. Though the current implementations of this device are not space-qualified, a direct path-to-flight for all components and design has been identified and work towards this is currently in progress.

The second device developed was an Integrated Optical Assembly (IOA), which is a monolithic optical device that serves as a passive basis choice measurement discriminator. It consists of beam splitters and reflectors glued together and aligned with fiber couplers so that light collected by the receiver can be sent into the device and photons exit one of four fibers that each represent a particular orthogonal measurement in one of two bases.

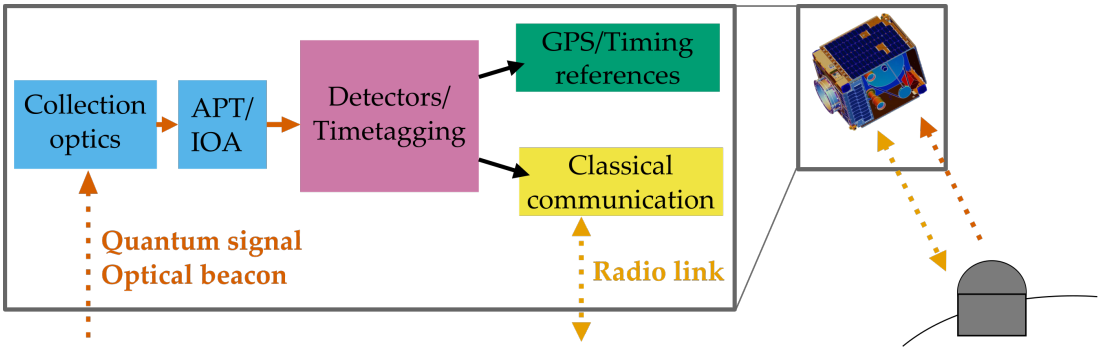



Figure 3.1: Functional diagram of quantum key distribution receiver (QKDR) receiver unit)

This device was assembled by a commercial partner and then was tested separately and in-situ with the rest of the experimental QKD apparatus.

The last device that will be discussed in this work is the Acquisition Pointing and Tracking (APT) unit. This device serves as a link from the photon collection telescope and the input port of the IOA and detectors. To reduce the stray light collected by the system, a 50 µm pinhole at the entrance of the IOA is used to reduce the field-of-view (FOV) of the entire optical system. Adaptive optics are used in many applications[129, 130, 131] to reduce loss or aberration in signals from telescopes to subsequent optical systems. The APT unit consists of a fast steering mirror that directs the signal photons into the IOA while using a beacon signal (collinear with quantum signal) on a quad sensor to provide spatial feedback on beam wander. We designed this device in conjunction with commercial partners who manufactured the prototype. We designed and constructed the mounting and did all of the testing (solo and in-situ).

**Contributions**

I designed the detector electronics with consultation from Vadim Makarov and Thomas Jennewein. I did the initial characterization. Further testing was done with Elena Anisimova and Catherine Holloway. I wrote the software that runs the detectors. Elena designed the mounting bracket and Zhenwen Wang helped with PCB tracing and assembly. I did the characterization and performance analysis of the IOA. I designed with Thomas Jennewein the mechanical structure for the receiver telescope/motor system, and the precision alignment mounting for the APT and I machined all the parts. I helped Chris Pugh, Brendon Higgins, Jean-Philippe Bourgoin, and Thomas Jennewein with design discussions and testing of the APT unit. Publications resulting from work in this chapter: [121, 132, 133].

## 3.2 Single photon detector unit

There are many commercially available devices that can be purchased to do single photon counting [134, 135, 136, 137]. As was discussed in Section 1.3, we decided to use the diode and thermal packaging from Excelitas and to design and construct our own readout circuit. This allows us much more freedom in customizing the actual detection signals as well as the physical size and power consumption. Customizing these aspects of a single photon detection unit also means that we can make compact and rugged packages of multiple units for our field testing.

The chosen primary detector candidate for the prototype is an Excelitas super low K avalanche photodiode (SLiK) that is expected to meet performance requirements such as dark counts and timing jitter derived for the requirements of this project [138]. The device contains four single-photon detectors with their sensitive areas coupled to four multi-mode fibers (MMFs). Photons are detected by absorption into the sensitive area of each detector. Electronics bias the detector sensitive area, achieving the necessary conditions (voltage, temperature) for single-photon sensitivity, and conditioning the detector output such that a clear pulse is emitted at each detection event. These low voltage differential signal (LVDS) pulses travel to the control and data processing unit (CDPU), where the time and detector from which they arrive is recorded and stored. We will now look at the custom readout electronics that were designed for these detectors.

### 3.2.1 Detector passive quenching circuit

Each detector is driven by a custom passively quenched single photon avalanche photodiode (SPAD) detector circuit. There are two main functions of this circuit: maintain single photon sensitivity (via a high voltage bias and temperature control), and discriminate detection events on the output across the diode. They operate in a free-running mode which means that they are able to detect photons anytime, provided they have recovered from the last detection. Passive quenching was chosen here as opposed to active quenching options due to the optical channel under consideration. The modeled channel was a free-space optical link from the ground to low earth orbit ($\sim$ 600km) with losses $\geq$ 35dB. For channels with losses this high mean that there will not be a strict need for high count rates at the detectors as most pulses will be lost in the atmosphere. Active queching primarily provides the ability to handle higher count rates at the cost of circuit complexity and power consumption, two properties that are not good for space hardware. Thus a passive quenching scheme was chosen.

A basic schematic for the electronics circuit is given in Figure 3.2. The high-voltage bias is connected through a quench resistor $R_q$ (baseline of 400 k$\Omega$), which limits the maximum steady-state current through the detector diode, thereby passively quenching the avalanche in the diode following a detection event.

For the ability to control and read parameters, individual digital-to-analog converter (DAC) and analog to digital converter (ADC) are used on each detector channel, and these ADCs/DACs are contained in a single chip, one chip per channel. This single component then mediates all of the communication for the channel over an inter-integrated circuit serial bus ($I^2C$) serial protocol to the CDPU. One $I^2C$ control line is shared by all four detector channels. This particular serial protocol was selected as it was the only protocol available for the single chip ADC/DAC that were selected. These chips were in turn selected for their high resolution and large address space. A separate circuit handles temperature readout of thermistors in the avalanche photodiode (APD) packages, and controls current through the thermoelectric controller (TEC) to stabilize the temperature. This allows for temperature adjustment and stabilization of the environment of the detector itself.

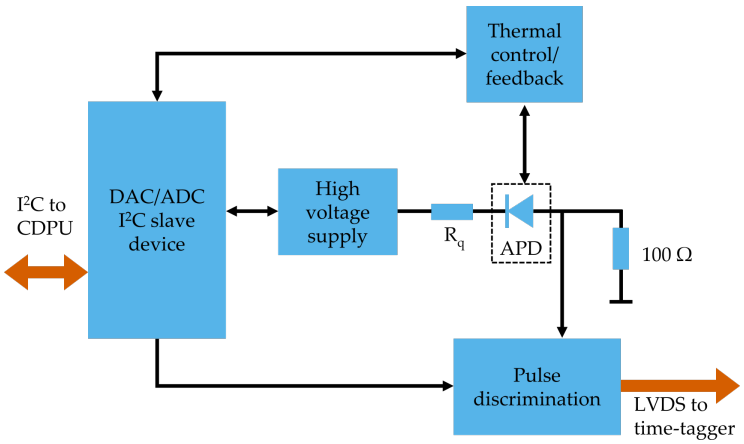



Figure 3.2: Functional diagram of passively-quenched detector electronics (one detector channel). Blue blocks represent parts in this circuit, and the wide orange arrows are communications to and from the detector unit.

The ADC/DAC chip controls the bias voltage of the SPAD and the threshold of the discriminator that identifies pulses from the SPAD. A high-voltage direct current (DC)/DC converter is used to reverse-bias the SPAD at a controllable voltage over its breakdown, so that the detection efficiency of the diode can be controlled and tuned. The ability to select the discriminator threshold is key to reducing jitter. The circuit diagram is given in

Figure 3.3 and the two-layer printed circuit board (PCB) layout in Figure 3.4. Any part identifiers referenced in the following sections can be found on Figure 3.3.

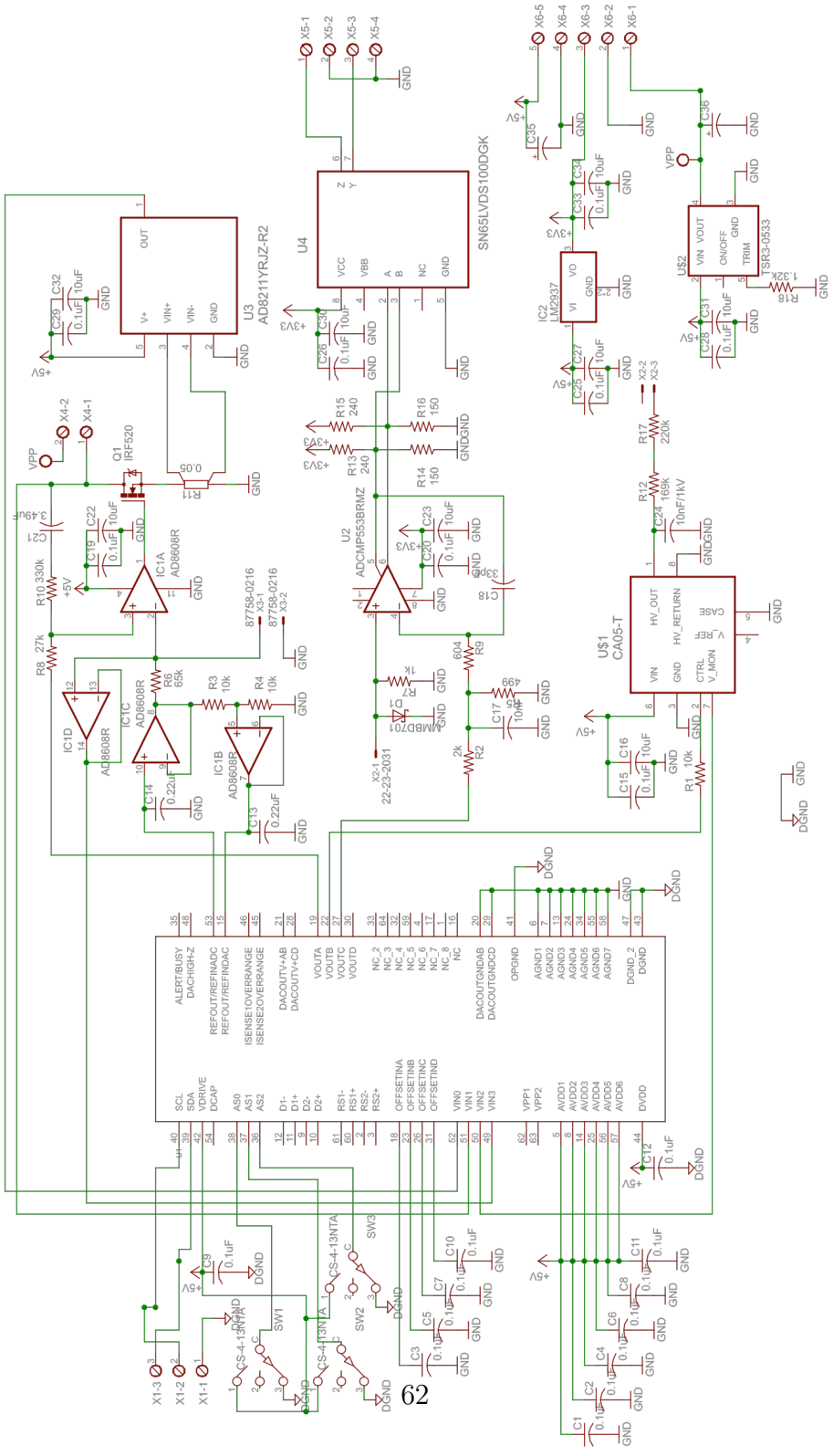


Figure 3.3: Circuit diagram of detector electronics (one detector channel).

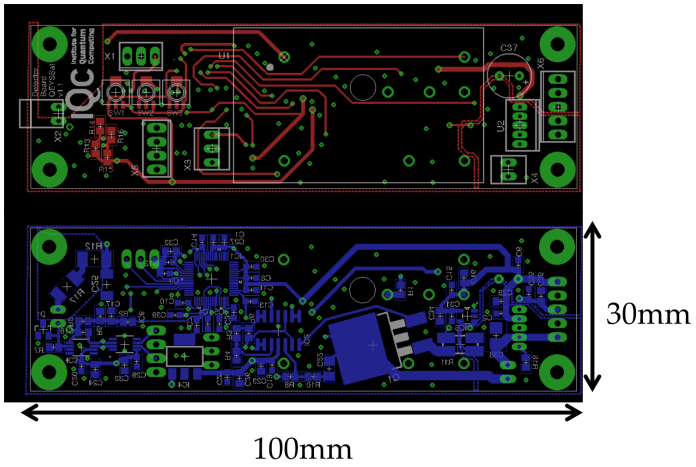



Figure 3.4: Detector Electronics PCB Prototype Design (Red: Top, Blue: Bottom)

The thermal control circuit consists of a current monitoring integrated circuit (IC) (instrumentation amplifier IC5), a transistor that throttles the TEC current (Q1), and an op-amp that controls the transistor (IC2A). The SPAD package has a built-in TEC and thermistor that are connected at X4 and X3 respectively. For monitoring the TEC operating conditions, there is a buffered readout of the TEC voltage and the current monitoring IC output to two of the ADC channels. The temperature is set by programming one of the outputs of the DAC, which goes to the non-inverting input of the current control op-amp. Meanwhile, the voltage at the inverting op-amp input depends on the thermistor resistance, so the set points for temperature are calibrated to the thermistor parameters.

The APD bias and readout circuit consists of a high voltage (HV) source and a high-speed analog comparator IC3. The comparator has a differential-output Positive Emitter-Coupled Logic (PECL), comparator to generate logic-level pulses from the diode current pulses, followed by a level converter (IC6) for converting the PECL levels to LVDS. The HV supply is a module (U1) with a programmable set point pin that is addressed by a DAC channel, and a readout pin for the output HV that goes to an ADC channel. The comparator detects pulses by monitoring when the signal from the diode crosses a threshold that is programmed by a DAC output. The output of the comparator is already a differential signal that just has to be buffered and converted to a different logic level standard, to interface more easily with other components and to isolate internal circuitry of the detector from possible electrical interference sources in the output differential line.

All control and monitoring functions on the board are performed by a large IC that has four DAC and four ADC channels, a stable 2.5 V reference, and the capability to interface

via the I$^2$C serial communication protocol. The DACs and ADCs inside the chip have 12-bit resolution with ranges of $0 - 2.5$ V and $0 - 5$ V respectively. Other components on the board include a 3.3 V voltage regulator and I$^2$C address switches. The regulator is necessary to power some of the ICs. The three-position address switches on three address pins allow for 27 possible I$^2$C base addresses selectable for each detector channel, allowing the sharing of I$^2$C bus address space with more than just the four detector channels, if necessary.

The TEC is powered separately from a 1.3 V power supply ($V$PP in the top right of Figure 3.3), and its power consumption depends greatly on the cooling state of the SPAD and the temperature difference between the heat sink and SPAD. During the initial cool-down of the APDs which is expected to be less than one minute, the TEC will be running at its maximum current. Power consumption while cooling down the diodes peaks at 2.05 W in that detector channel. After the initial cool-down, the steady-state power consumption stabilizes at a lower value that depends on the heat sink temperature and the SPAD set temperature. Assuming the heat sink of the TEC is at room temperature (20°C) for the ground prototype, the steady-state power consumption per TEC is on the order of 1 W. To reduce the initial power consumption of the TECs, cooling is switched on one channel at a time.

### 3.2.2 Quad detector assembly

The physical layout for the complete detector assembly contains four adjacently placed single detector channels, as shown in Figure 3.5. Each detector is coupled to a MMF in a compact fashion. The fiber-detector coupling assembly is provided by Excelitas. Four SLiK detectors and electronics boards are mounted on a single bracket machined of aluminum alloy. The bracket is anodized to improve the surface hardness and durability during testing operations. Twelve cut-outs are made in the bottom of the aluminum bracket to decrease its mass.

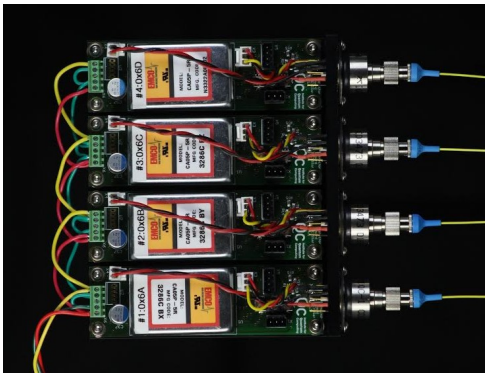


Figure 3.5: Photo of the QKDR detector package. Four SLiK APDs, each with an incoming optical fiber (right) and electronics PCBs, mounted on a monolithic aluminum alloy bracket. Photo by Scott McManus.

Thermal dissipation of the TEC hot plate in the SLiK packages is implemented by tightly mounting the packages to the aluminum bracket, which acts as a heat sink. Surface anodizing is removed at the SLiKs' contact areas to allow good thermal conduction. An extra heat sink with fans may optionally be attached under the bracket. In this case, the height of the assembly will increase by the thickness of the heat sink (e.g., about 30 mm). The main PCB layout constraint is the large package size of the HV supply mounted on the upper side of the board. Most other components are on the bottom of the boards. The channels operate independently, with the exception of the common power and $I^2C$ lines. Each channel has one fiber coupler connector on the outside of the vertical section of the bracket, and an LVDS signal line consisting of two wires for the differential signal and two ground wires (internally connected to the power ground on the PCB).

The common connections to each board are the +5 V and +1.3 V power supply lines, power supply ground, and the two-wire $I^2C$ serial communication line with its own ground wire (internally connected to the power ground on the PCB). The power and power ground are connected to screw terminals (X6 in Figure 3.3) at the narrow edge of the board opposite to the SLiK detector head. The ground planes of the board are connected to the standoff screw pads and provide grounding for the bracket. The $I^2C$ connector (X1) is on the top of the board close to the right side of the detector. X5 is the LVDS connector, located as close to the comparator as possible to reduce possible impedance mismatch. The SLiK SPAD package pins are wired to the PCB in several places: SPAD pins are connected at X2, the thermistor and case ground at X3, and the TEC at X4.

### 3.2.3 Detector-CDPU Interface

The main detector output for the detection of photons is a LVDS pulse. The connector for each channel has four wires: two ground wires and two wires for the differential signal. The latter must be terminated at the CDPU interface with a 100 Ω resistor connected in between the differential wires. The main control interface is a standard $I^2C$ communication protocol, where the base address of each detector channel (or slave devices in the protocol) is set by the three physical switches on the channel PCB. Control and readout of the parameters is done via byte-wise binary communication to the DAC/ADC IC. The CDPU will be the master device or the hub, and pull the communication lines up to 3.3 V. To initialize a channel, after it has 5 V power, an initialization command is sent to turn on the appropriate DAC and ADC channels and reference voltage configuration. Following this initialization sequence, commands can be sent to write values to each of the four DAC channels and read from the four ADC channels. A table of example command strings in hexadecimal can be found in Table 3.1. There are four, 12-bit monotonic DAC channels

Table 3.1: Sample table of commands used to control the detector unit.

| Description (Read/Write) | Command |
|---|---|
| Initialization (w) | 0A100900F0 |
| Set DAC channel N, N = 0,..,3 (w) | 0N [12-bit value to be set] |
| Read ADC channel N, N=0,..,3 (w,r) | 00 0N 01, read |

with each detector, which are configured to control the following three parameters:

1. detector diode bias voltage,
2. comparator threshold for the avalanche detection,
3. temperature set point for the cooling system.

Each channel of the DAC is configured to have outputs from $0 - 5$ V, with resolution of approximately 1 mV per step. The bias voltage for the detector diode is set by sending a voltage of $0 - 2.048$ V to the control pin of the high voltage supply. To set the comparator threshold, the DAC is set to apply a voltage proportional to the threshold desired, and a resistor network ensures the threshold value is correct at the negative input of the comparator. The desired temperature for the diode is set similarly through a resistive divider and to the positive input of the comparator controlling the TEC current. The last channel of the DAC is unused. The ADC monitors the following four parameters with

12-bit resolution: the TEC current, the TEC voltage, the bias voltage on the diode, and the temperature of the diode.

All inputs are configured to read from $0 - 2.5$ V, with resolution of approximately 0.6 mV. The TEC current is measured with a small shunt resistor. The voltage for the TEC is buffered and read directly. A readout pin on the high voltage supply provides a voltage from $0 - 2.048$ V, giving the readout of the bias voltage. Lastly, the temperature of the diode is monitored with a 10 kΩ thermistor in the package of the diode.

The detectors are controlled by a python program that can be found in Appendix B. A screenshot of the program can be found in Figure 3.6. The program was run on a Raspberry Pi computer, as the $I^2C$ interface for the CDPU was not functioning.

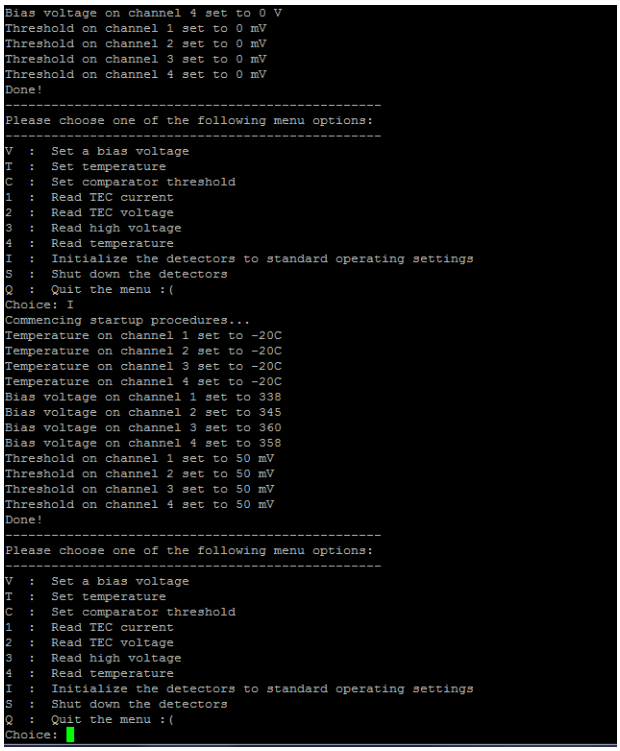



Figure 3.6: Screenshot of the detector control code menu. Python source code can be found in Appendix B.

### 3.2.4 Unit integration and validation

Overall, the detector unit meets all requirements specified in [138] barring the technical issues with the $I^2C$ interface, which we work around by using a Raspberry Pi computer to control the detector unit instead of the CDPU. These requirements specific to the detectors are reproduced in Table 3.2.

Table 3.2: Detector unit requirements from QKDR project [138]. The last column indicates whether the hardware developed met the requirement. The Y* indicated the detectors performed to the requirement, but the power draw of the CDPU was not estimated correctly when developing the requirement. Therefore the combined power draw was a bit too high, but this was not a failure of the detector hardware. Other referenced requirements for QKDR can be found in [138].

| ID | Title | Requirement | Satisfied |
|---|---|---|---|
| QKDRD-001 | Quantum Efficiency | Each detector shall have a quantum efficiency of >23% at the signal wavelength. | Y |
| QKDRD-002 | Dark Counts | Each detector dark counts shall not exceed 200 counts per second per detector after one year nominal mission equivalent of radiation exposure. | Y |
| QKDRD-003 | Timing Jitter | Each detector shall have a timing jitter that does not compromise the required system clock accuracy [QKDR-006]. | Y |
| QKDRD-004 | Configuration | QKDR detector assembly shall include four detectors, each with independent optical inputs and signal outputs. | Y |
| QKDRD-005 | Power Draw | QKDR detector assembly power draw, in concert with CDPU power draw [QKDRB-011], shall be compatible with the ORA power draw specified in [QKDR-011]. | Y* |
| QKDRD-006 | Volume | QKDR detector assembly volume, in concert with optics volume [QKDRO-001], shall be compatible with the ORA volume specified in [QKDR-008]. | Y |
| QKDRD-007 | Mass | QKDR detector assembly mass (in concert with [QKDRO-002] and [QKDRB-002]) shall be compatible with the overall system mass specified in [QKDR-010]. | Y |
| QKDRD-009 | Survivability | Each detector shall not be damageable by illumination of the Sun through the optical assembly (order 1013 photons/s at the detector) or design must be modified to prevent this. | Y |
| QKDRD-010 | Saturation | QKDR detector assembly photon counting saturation level shall be >80,000 counts/sec. | Y |
| QKDRD-014 | Control | QKDR detector assembly operating state and thermal conditioning shall be controlled by, and report to, the CDPU, in a manner compatible with the CDPU. | Y |
| QKDRD-016 | Output Signal | QKDR detector signal outputs and physical transport lines shall maintain high-precision timing of [QKDRD-003] and be compatible with the CDPU. | Y |
| QKDRD-017 | Cooling | Each detector shall possess active thermal control of the sensitive area. | Y |

#### Quantum efficiency

The quantum efficiency, i.e. the probability that an incident photon will result in a macroscopic pulse that can register in the time-tagger, is primarily dependent on the bias voltage that is applied. A higher bias voltage can increase the quantum efficiency, however it can also increase other effects such as dark counts, so the optimal value must be found. The quantum efficiency was the first parameter measured from the diodes when the detectors

were first assembled. To begin with, the breakdown voltage stated on the device test sheets was verified by watching the output of the diode as the bias voltage across them was ramped up.

The bias voltage was ramped (above the breakdown voltage) to characterize the efficiency as a function of bias, called overvoltage. The results are shown in Table 3.3. This was done by using a pulsed laser source attenuated to single photon level and comparing the counts per second to what the detector reports. The frequency chosen was $\sim 30$ kHz, low enough to avoid saturating the detectors. To avoid saturating the detectors, a passive probe was placed near the diode readout circuit to observe the detection pulses by capacitively coupling to the circuit. We could see from the shapes of the pulses that the internal capacitances were charged up again before the next detection. The actual saturation rate is measured in Section 3.2.4.

We choose a standard operating overvoltage of about 28 V, where we find efficiencies tend to be better than 50% in each detector. This is lower than the $\sim 60\%$ quoted for the signal wavelength, but the operating conditions may not have been the same. In any case, our measured efficiency is well above the 23% requirement [QKDRD-001], but does not meet the goal 80% [QKDRD-G-001]. (It should be noted, however, that this high a quantum efficiency is unlikely to be achievable with anything but the most state of the art Si SPADs [139, 51]).

Table 3.3: Final measured quantum efficiency of the 4 detector channels measured at different bias voltages (volts over the breakdown voltage).

| Overvoltage [V] | Detector 1 | Detector 2 | Detector 3 | Detector 4 |
|---|---|---|---|---|
| 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% |

### Dark counts

Measuring the dark counts of the detectors is a straightforward procedure. The detectors are powered on and the cooling is allowed to run for sufficient time to stabilize the temperature (approximately 30 seconds). Then the comparator and bias voltage are set and time tags are collected with the rest of the setup as it would be for data collection (i.e. covered and lights off in the room). The requirement [QKDRD-002] is less than 200 dark counts per second on each detector channel, and the detectors averaged 24 counts/s. This

is under optimal operating conditions of $-20°C$, 28 V over the breakdown voltage and a 50 mV avalanche detection threshold. There is, however, a much larger operating range of temperatures, biases, and detection thresholds that allow for this requirement to be met (see Table 3.4).

Table 3.4: Measured dark counts as a function of temperature and bias voltage over breakdown. Detection threshold is 50 mV for all tests. Colored cells indicate an set of operating conditions that meets the requirement of $< 200$ dark counts per second.

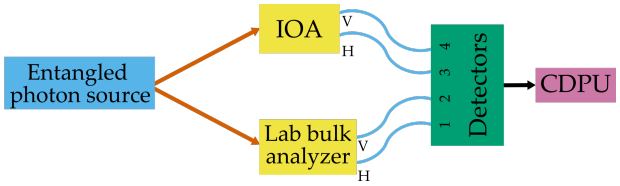
| Detector 1 | | | | Detector 2 | | | |
|---|---|---|---|---|---|---|---|
| Temp (C) | 7 V | 14 V | 28 V | Temp (C) | 7 V | 14 V | 28 V |
| -20 | 5 | 16 | 35 | -20 | 2 | 4 | 7 |
| -10 | 14 | 50 | 105 | -10 | 10 | 15 | 28 |
| 0 | 50 | 136 | 278 | 0 | 30 | 52 | 88 |
| 20 | 341 | 954 | 1840 | 20 | 250 | 516 | 864 |
| Detector 3 | | | | Detector 4 | | | |
| Temp (C) | 7 V | 14 V | 28 V | Temp (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 |

### Timing jitter

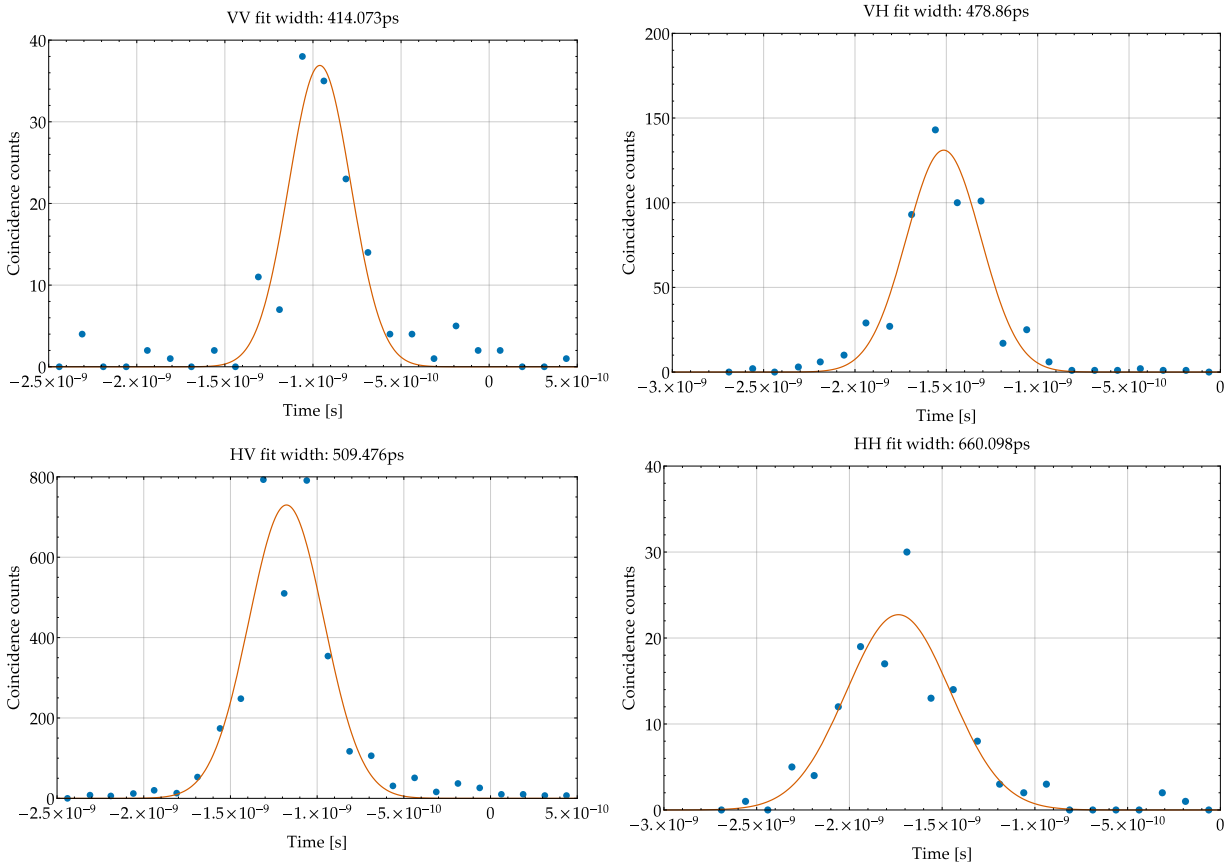
The timing jitter of the detectors is a trickier parameter to measure. They cannot be measured in isolation, and need at least a source and some sort of time tagging electronics. These other devices have their own jitter and the jitter measured in a setup is really the combined jitter of all the devices. The standard measurement setup is a splitter and a trigger detector with known jitter is used to correlate the detections in the unknown detector. By knowing the jitter of the laser pulse source and the triggering detector it is possible to de-convolve the contributions of these sources and find the jitter of the unknown detector.

Here, we use an entangled photon source and split the pair and send each photon through a passive polarization analyzer (see Figure 3.7a). The H and V channels of both polarization analyzers are plugged into the four detector channels on the QKDR prototype. Since all signals are compared across the same time tagger, the GPS receiver and timing

alignment software are no longer needed for synchronization. In addition, the timing jitter of our photon source is very small: from Heisenberg uncertainty, the bandwidth of our entangled photons 0.23 nm leads to an estimated time jitter in the arrival of the photons of order 1 ps.

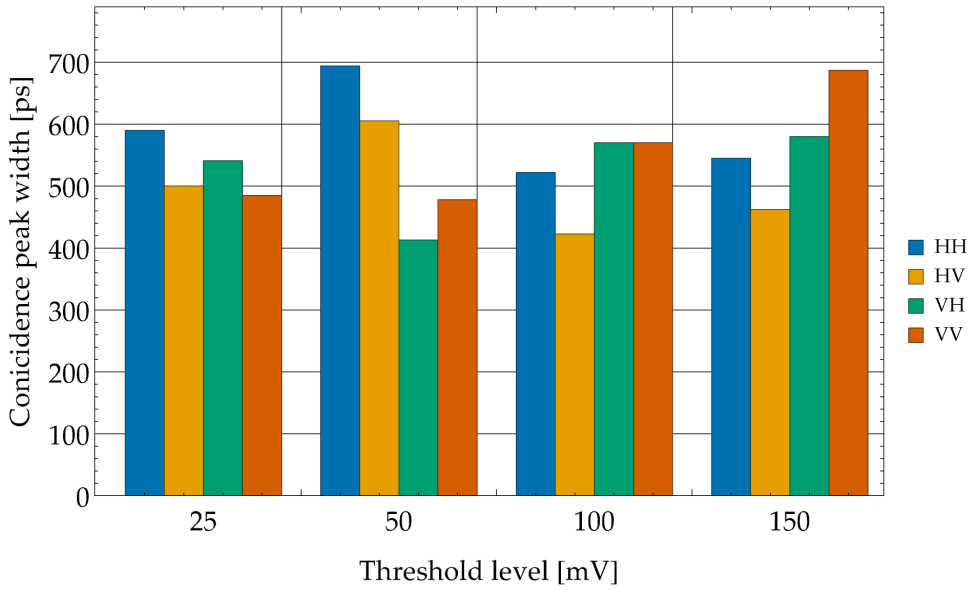



(a) Setup for the timing jitter measurement. The H and V channels of both Alice's and Bob's polarization analyzers were connected to the four detectors (with MMF) of the QKDR.

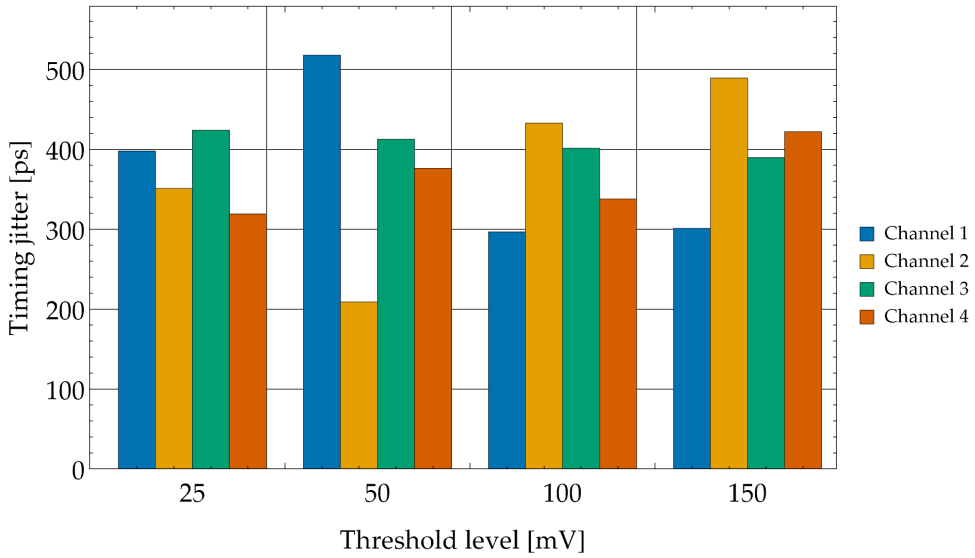



(b) Typical timing histogram and Gaussian fits for relative time measurements between the Alice and Bob channels. The x-axis is time delay in seconds and the y-axis is the number of coincident counts.

Figure 3.7: Testing setup and jitter measurements for the quad detector array.




(a) Timing histogram widths obtained from Gaussian fits for timing histograms between Alice and Bob detector channels.




(b) Individual timing jitters for each channel estimated from Gaussian fits between Alice and Bob pairs and solving for individual timing uncertainties.

Figure 3.8: Timing jitter measurements for detector combinations and individual detectors.

Histograms of the differences in times of arrival between each pair of entangled source output analysis channels are constructed, and these histograms are fitted to Gaussian distributions. The widths of these peaks are reported in Figure 3.8a. For all channel combinations and threshold voltages, the observed width is below 700 ps, and is often below 600 ps. This is likely a true measure of the timing jitter of our system, given that $600 - 700$ ps is several orders of magnitude above 1 ps, the timing jitter of the entangled photon source.

Now since these are 4 unknown jitter sources, what we have looked at so far are convolutions of the jitter of two detectors at once. Now, we can easily tell that the convolution is not Gaussian and in fact timing jitter is not Gaussian [140]. However it is standard to model them as Gaussian so that it is easy to deconvolve the distributions. However deconvolving Gaussians that are only approximate makes it tricky to know how to isolate the jitter from each detector. If we naively assume the detectors are identical and independent, we can try to separate them in the following way:

$$\sigma_{13}^2 = \sigma_1^2 + \sigma_3^2 \tag{3.1}$$
$$\sigma_{14}^2 = \sigma_1^2 + \sigma_4^2 \tag{3.2}$$
$$\sigma_{23}^2 = \sigma_2^2 + \sigma_3^2 \tag{3.3}$$
$$\sigma_{24}^2 = \sigma_2^2 + \sigma_4^2 \tag{3.4}$$

$\sigma_{13}^2$ is the variance of the Gaussian fit to the jitter of detectors 1 and 3 and $\sigma_1^2$ is the variance of the jitter of detector 1. If this system is solved for the fitted widths found for each threshold setting we get the histograms in Figure 3.8b.

Separating these distributions over each channel, the combined timing jitter of the CDPU and detectors is $425 - 500$ ps, compliant with the overall system timing accuracy requirement of 0.5 ns [138], and thus satisfying the detector jitter requirement [QKDRD-003]. Removing the contribution of the CDPUs minimum timing resolution, this leaves the detectors with a timing jitter of $417 - 493$ ps, which is consistent with the observed detector timing jitter found in the radiation testing [141].

### Dead time

Because the single photon detectors are operated using passive quenching, they will have a finite recharge time effectively determined by the capacity of the circuit at the cathode (this capacitance is of order pF, due to stray capacitances in the devices as well as the circuit construction), as well as the value of the quench resistor (400 k$\Omega$). The recharging

of the SPAD after a detection event can be modeled as a simple RC circuit. The voltage will increase exponentially after a detection event as [56, 142]:

$$\Delta V(t) = V_0 \left(1 - e^{\frac{-t}{\tau_A}}\right) \tag{3.5}$$

where $\tau_A$ is the time constant, and $V_0$ is the asymptotic voltage level above breakdown. We must note that detector efficiency is an exponential function of the bias voltage:

$$\Delta P_d(t) = V_0 \left(1 - e^{\frac{-\Delta V(t)}{V_c}}\right) \tag{3.6}$$

where $V_c \sim 8.5$ V is a voltage coefficient, for the SLiK diode used here. In combination, the effective dead time of the detector will be due to the gradual increase of detector efficiency, which follows a doubly exponential behavior:

$$\Delta P_d(t) = V_0 \left(1 - e^{-\frac{V_0}{V_c}\left(1 - e^{\frac{-t}{\tau_A}}\right)}\right) \tag{3.7}$$

From analyzing the times between consecutive detection events, we are able to determine the time constant of each detector. For the data taken on 18 December 2014 (over 200 sec) the following timing distribution was observed, shown in Figure 3.9. The data was collected as a histogram of the delay from the designated trigger detector count to when the other paired detector clicked. This histogram was then integrated to produce the curves shown in Figure 3.9.

In order to calculate an expected saturation behavior of the detectors, we use the above dead time model as well as the time distribution of photons following Poisson distribution:

$$\Delta P\left(\Delta t\right) = re^{-r\Delta t} \tag{3.8}$$

where $r$ is the rate, and $\Delta t$ is a certain time interval.

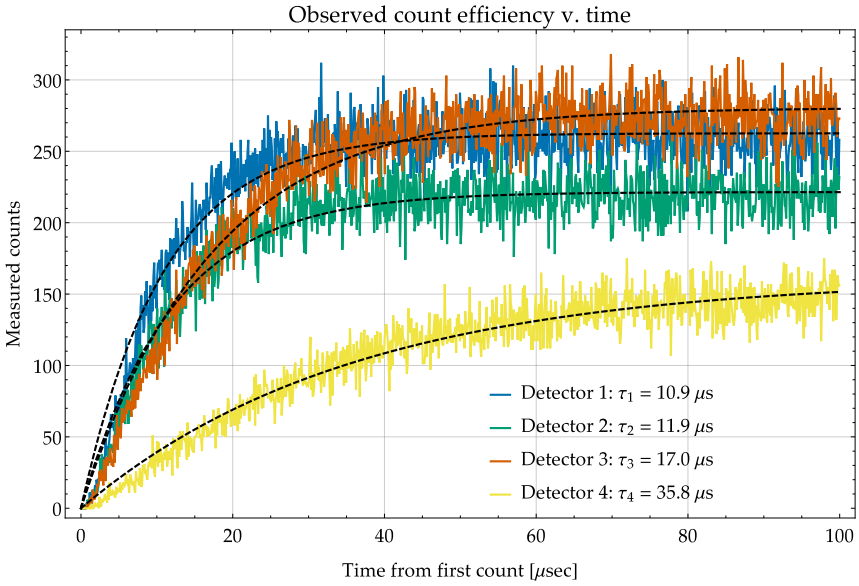



Figure 3.9: Measured distribution of time delay after a certain detection event. The lines show a fit of the model from (3.5) to the data. $\tau_1, \tau_2, \tau_3, \tau_4$ represent the recharge time constants for each detector.

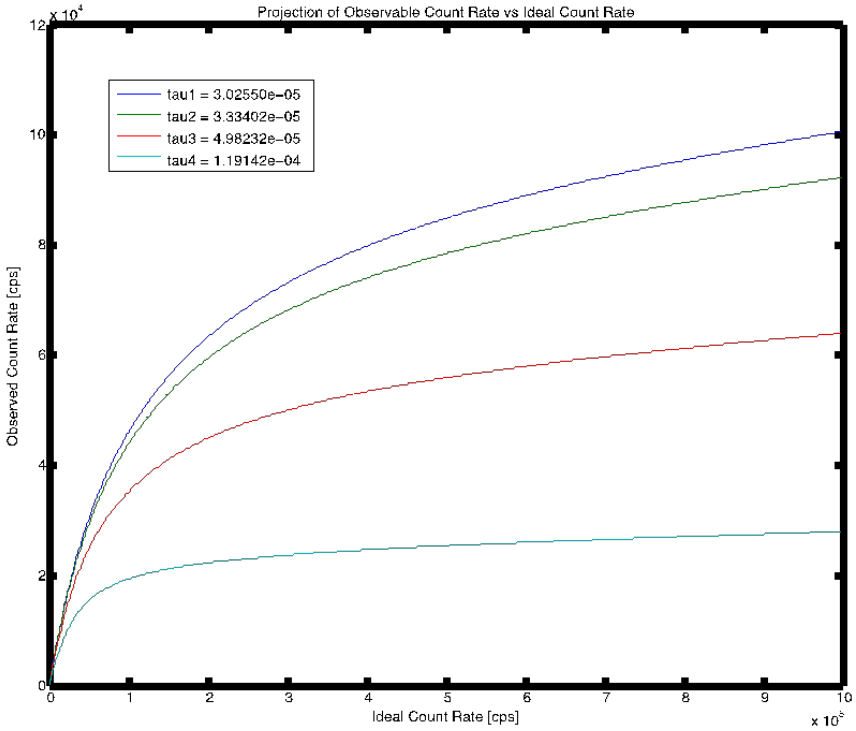



Figure 3.10: Projected saturation behavior of the QKDR detectors. The observed count rates are shown as a function of present count rate. At input counts of about 20000 counts/s, the four detector graphs roughly overlap.

Because the Poisson distribution has a higher likelihood of events in short time intervals, the effective dead time of the photon detector will lose a larger fraction of events as the rate increases. The resulting behavior is shown in Figure 3.10. From this prediction we can determine that in combination, the QKDR detectors will saturate well above 20 kHz each, which means the total requirement of 80 kHz [138] is reached.

We note that the dead time observed here is significantly longer than the dead time observed during other detector tests. It is possible that some particular differences in the PCB layout or choice of resistors caused this change. Certainly it is clear that better performance should be achievable with some relatively small modifications to the detector assembly electronics [56].

### Mechanical and power performance

The overall size of the detectors assembly (four SLiK detectors, PCBs, and bracket) is 128 mm × 107.5 mm × 29 mm. This is well below the allotted 150 mm × 150 mm × 200 mm for the electronics and optics [QKDR-008] [138] . The weight of the assembly is estimated to be 0.5 kg, much less than the goal of 5 kg [QKDRD-G-007] [138].

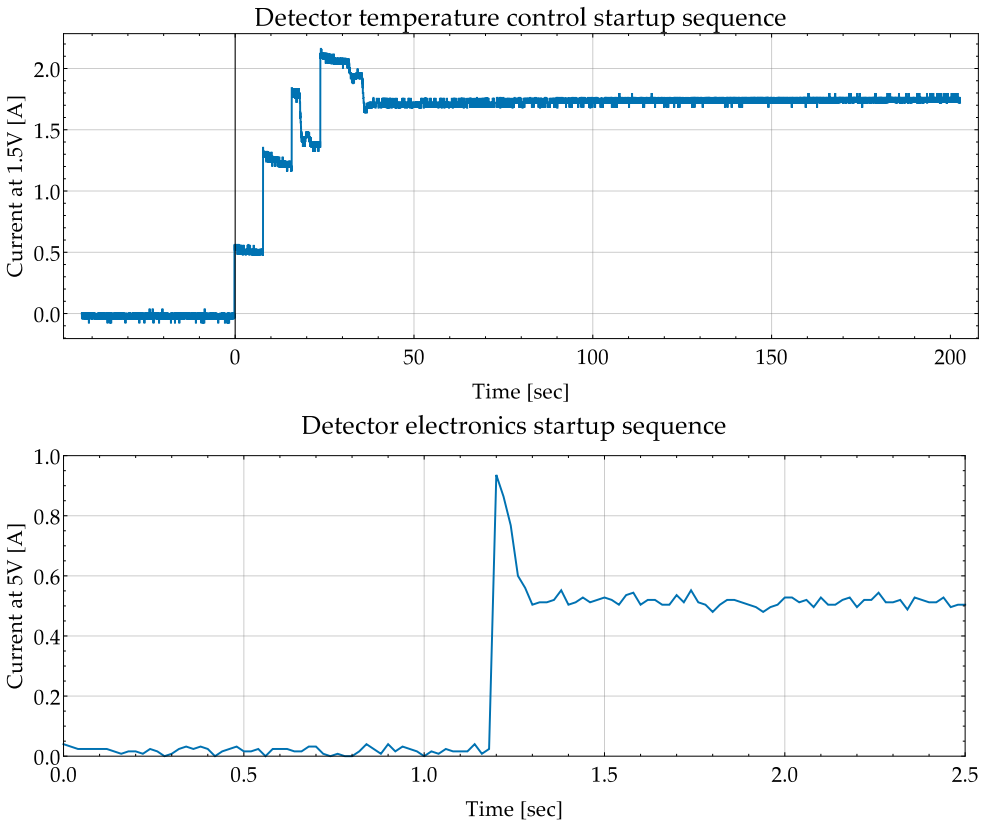



Figure 3.11: Power draw from start-up of the detector assembly. Measurements taken with a current probe (100 mV/A). The peak detector electronic current was 0.936 A for approximately 80 ms.

To measure the power draw of the detectors and cooling systems, a current clamp was attached to the individual power lines. Plots for the detector electronics and detector cooling current draws at start-up can be found in Figure 3.11. Note on the detector control electronics there is a short power spike with a peak of 5W and a width of less than 1 sec.

This is due to a manufacturer design defect in the devices that causes the device to generate a brief spike of bias voltage on power-up. Following this transient spike, the detector draw after start-up is less than 3 W.

The start-up trace of the detector temperature control electronics shows the four different detector TECs initiating and cooling down from room temperature in sequence. Variations for each unit could be due to thermal coupling or manufacturing differences. The detector cooling is not included in the budget as it is highly dependent on the environment (our lab is not representative of the flight-like environment).

With incident photons producing a 46 kHz count rate, the measured detector power draw was 2.31 W. Thus, the goal power draw of 2.5 W average and 3.5 W peak [QKDRD-G-005] would be achieved if the high-voltage supply was not producing the transient spike at power-on.

Table 3.5: Detector power draw at different stages of operation. All power values measured in W.

| Device | CDPU | Detector Electronics | Detector Cooling | Totals (No Cooling) |
|---|---|---|---|---|
| Start-Up (average) | 5.08 | 2.13 | 2.07 | 7.21 |
| Start-Up (peak) | 6.87 | 4.68 | 3.15 | 11.55 |
| Idle (average) | 4.02 | 2.05 | 2.67 | 6.07 |
| Idle (peak) | 4.70 | 2.28 | 2.76 | 6.98 |
| Dark Counts (average) | 4.18 | 2.47 | 2.72 | 6.64 |
| Nominal Count Rates (average) | 4.54 | 2.31 | 2.86 | 6.85 |
| Processing (average) | 4.56 | n/a | n/a | 4.56 |

### Path-to-Flight Assessment

As discussed previously, the purpose of this attention to design detail is to make the hardware developed as close to what could be directly used in a space mission. However, it is not possible to make a prototype space-qualified in one fell swoop; the hardware discussed in this chapter that is not space-qualified will be evaluated to establish a path-to-flight for the device. These assessments can then be used to determine next steps required to make the hardware ready for space flight. We discuss a few of these now.

The detector diodes are sealed in gaskets that will leak over time, and the reduced pressure in the package can allow electric discharge due to the high voltages involved[143]. A leakage rate for flight applications is usually specified for space-qualified devices, and it will need to be analyzed for very long durations as it will affect the overall life expectancy of the detector package. Depending on the package, $5-10$ years may be a ballpark figure for a reasonable lifetime, however, a more detailed assessment will be needed. As an example, ice, cloud and land elevation satellite (ICESat) was a three-year mission that survived for five. For Quantum Encryption and Science Satellite (QEYSSat), a one-year mission baseline requirement with a two-year extended mission goal should therefore be achievable.

Optimizations could be made to improve the detector efficiency beyond that of the off-the-shelf SLiK devices selected. For example, with specifically selected anti-reflection coatings on the diode, lens and window, tailored for the signal wavelength, and by selecting a thicker die, it would be feasible to reach 70% quantum efficiency, quite close to the 80% minimum efficiency goal [QKDRD-G-001]. Of course, doing this has trade-offs: different coatings would need their own testing for flight-readiness, and a thicker die is likely to increase dark counts and timing jitter.

The $I^2C$ interface between the detector board and the CDPU was chosen for convenience. For a flight version, this interface could be replaced by one more appropriate for the bus environment. For example, if the bus were to provide information to the CDPU over a controller area network bus (CAN) interface, then also utilizing a CAN interface at the detector assembly might make sense.

Adjustments to improve signal quality of the LVDS pulses can be made. At the same time, the components identified as needing replacement for flight compatibility would be addressed. Details of these path-to-flight considerations for the detector assembly can be found in [144]. Additionally, to maintain the power budget for flight hardware, a voltage supply that does not exhibit a transient power spike at power-up would be selected.

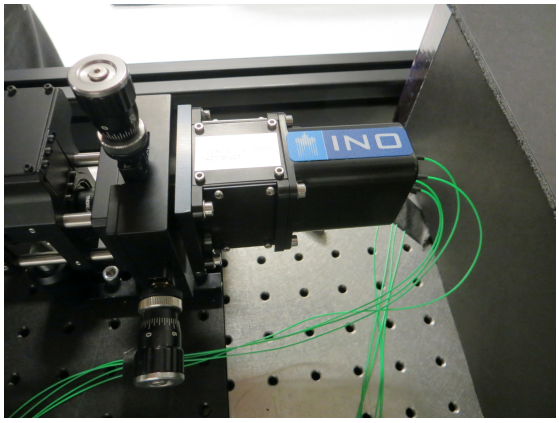
The chosen detector, Excelitas SLiK, has previously flown in space in the Geoscience Laser Altimeter System (GLAS) mission, however it showed a large increase of the dark count rate during the mission because of space radiation [145, 146]. Addressing the technical risk of radiation susceptibility of the chosen detectors is a primary focus of this project; testing and mitigation assessment was done independently of the design and construction of the prototype, the results of which can be found here [141]. The results of this study were that the approach of using thermal annealing to reduce dark counts in the device when not in use, was successful and should ensure that a $\sim 2$ year mission is possible.

## 3.3 Integrated optical assembly

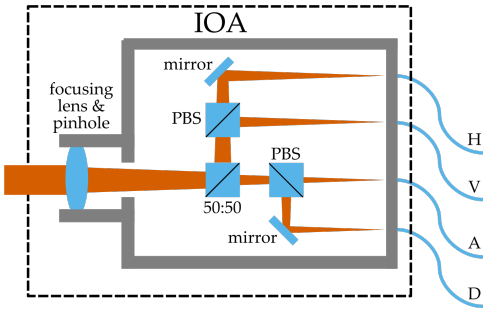
### 3.3.1 Bulk optics and polarization

Any QKD system that encodes quantum states using polarization will need a polarization analyzer of some sort. These devices serve the purpose of both selecting Bob's measurement basis and making the subsequent measurement. They can be passive basis choices (basis chosen by a choice at a beamsplitter) or active basis choices (basis chosen by externally generated random bit string and an active optical element), each with different advantages and disadvantages. Passive basis choices are easier to implement practically, but introduce slight biases that have to be corrected for (no splitter is exactly 50:50). Active basis choices can avoid the locality loophole [147] for locality tests and allow independent sources of randomness to be used. Since the goal for our space QKD link is to have a simple and robust devices on a space payload, the passive basis choice was selected. Additionally, in the case of QKD experiments we generally assume that quantum mechanics is correct. As long as double click (more that one detector clicking per expected input) are not thrown out and are instead randomly assigned one of the two values [148], it does not matter whether the basis is chosen activly or passivly.

A standard construction for a passive polarization analyzer in the lab consists of beam splitters, wave plates, and fiber couplers all on multi-axis stages. This can provide many degrees of freedom for coupling the light from the entrance to fiber-coupled or free-space detectors. However, in an outdoor scenario this is too many degrees of freedom to make stable. The approach for this device is to remove all the degrees of freedom internally in the analyzer and glue all the components together. The end result is a wonderfully compact and stable device that can be seen in Figure 3.12a.




(a) IOA for analyzing polarization of input photons.




(b) Conceptual layout for the internal function of the IOA. The fibers then each correspond to a particular measurement outcome as labeled on the right. One of the polarizing beamsplitter cubes (PBS) is rotated 45° to measure in other basis.

Figure 3.12: The Integrated Optical Assembly device.

The IOA consists of a focusing lens followed by a non-polarizing beam-splitter cube. Then two polarizing beam-splitters, with one cube rotated by 45° relative to the other (see Figure 3.12b), provide the measurements for each basis arm. One polarizing cube beam-splitter thereby discriminates between horizontal and vertical polarizations, while the other polarizing beam-splitter, oriented at 45° around the direction of propagation, discriminates between diagonal and anti-diagonal polarizations. Additional polarizing beam-splitters or right-angle prisms are added to fold all four exit beams in the same direction, and increase isolation if necessary.

Pairing cube beam-splitters in such a way is a standard technique to ensure high-contrast output in both transmitted and reflected arms. The focusing lens re-images the pinhole on four multi-mode fibers with a focal length of 31 mm. MMF are attached to the outputs of the cube beam-splitters. These fibers are then used to direct the light to the detectors, and are labeled as to the measurement outcome they represent: horizontal (H), vertical (V), diagonal (D) and anti-diagonal (A). The front-end interfaces with the telescope optics and the APT through the pinhole.

### 3.3.2 Unit integration and validation

In order to test the IOA unit that was built, we use the setup shown in Figure 3.13. Linearly polarized light from a laser at 785 nm was collimated from a polarization maintaining fiber and input to simulate light coming from the telescope and APT components. Then a half-wave plate was used to rotate the polarization, and a subsequent polarizer was used to ensure the purity of the polarization state input to the IOA. Coupling was achieved with full spatial degrees of freedom as well as translation for the IOA in the focal plane and micrometer control of the lens along the optical axis. For measuring the power in the output fibers from the IOA, a series of fiber bulkheads were used, with the same power meter head used to measure each of the outputs. Using a single power meter eliminated the need for calibrating the readings of multiple power meters and aided in keeping the relative power measurements accurate. Input test powers were on the order of 3 mW, to ensure sufficient resolution of the measured parameters.

Figure 3.13: Setup used for testing IOA properties.

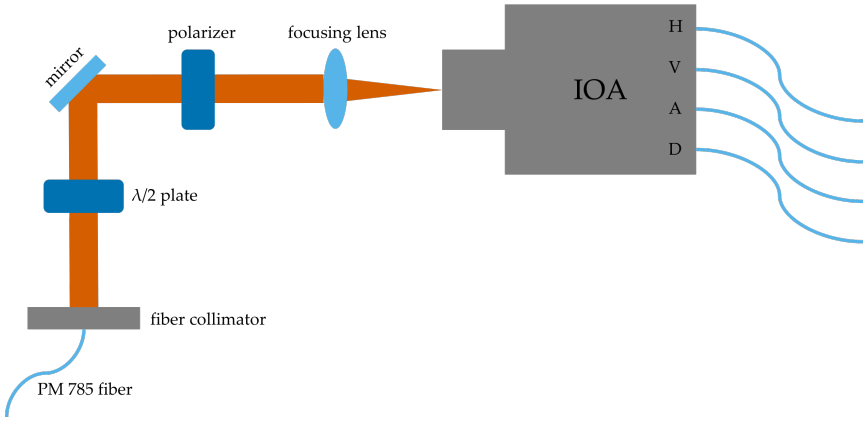
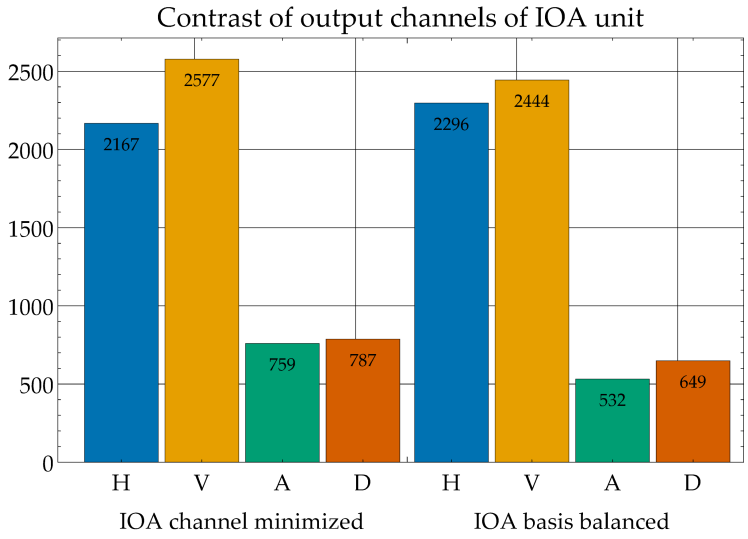


Figure 3.14: Measured polarization contrast results for testing the IOA. Contrast here is defined as the ratio of power collected in the channel of the state that was sent to the orthogonal collection mode. For example if state H was sent, the ratio of the power in H to the power in V at the detectors. Note in all optimization methods, the contrasts are above the 500:1 goal. The H/V basis was better than the A/D basis due to internal alignment.




The goal of these tests was to validate the requirements for channel contrast [QKDRO-005, QKDRO-G-005] [138], basis choice bias [QKDRO-004, QKDRO-G-004] [138]and overall device transmission [QKDRO-009] [138]of the unit. For this device, the average transmission found was 74.06%, which is sufficient for the 63% requirement. The bias of the basis choice was found to be on average 49.29% in the H and V basis to 50.81% in the A and D basis relative to the total power measured in all the arms of the IOA. This is very close to the target goal of 50:50 and well within the requirement of 60:40.

Lastly for the optical testing the contrast of the channels was measured in two ways: the transmission of one channel was minimized to give maximum contrast in one basis, and to target one channel transmission by balancing the power in the opposite basis. In Figure 3.14 it can be seen that the contrasts in the channels are always greater than the requirement of 100:1 as well as the goal value of 500:1.

The other requirements of the IOA unit were the mass and the volume of all the optical components. The overall mass was 320 g and volume of 48.2 mm $\times$ 56.8 mm $\times$ 120 mm, which meets the goal of 3 kg, and almost the goal of 60 mm $\times$ 60 mm $\times$ 110 mm, but is certainly the requirement of the overall payload volume compliance.

### Path-to-Flight Assessment

Now that the device and performance testing has been described, the space readiness of our device can be evaluated. With the IOA there are a few main categories which would need further evaluation or different approaches.

The first is the use of adhesives and coatings in the unit and the vacuum environment it will operate in. Many materials will outgas when put under vacuum and this will contaminate the vacuum environment [149]. Thus for space compatibility, the adhesives for attaching the beam splitters and prisms together, to the housing, affixing the alignment of the fibers, and the anti-reflection (AR) coatings on the optics all would need to be space-qualified. Many of the materials currently used do meet most of these requirements, but the AR coating would require further testing to verify its suitability. The materials that the fiber jackets and strain relief are made of are currently not vacuum compatible, but could be replaced with Teflon which can be space-qualified.

Another area for inspection is where the MMF exits the APT. The length of the fibers were chosen to facilitate work in the laboratory. Such long fibers would be unnecessary mass in a flight version, and would be reduced. Fibers also can be adversely affected by the space radiation environment. One possible effect is photo-darkening, which would have to be evaluated considering the radiation dosage and the mission duration. If the device accidentally faced the sun, in the worst case it will be subjected to 685 W of solar radiation (assuming perfect capture by the APT over all wavelengths) focused into the IOA. This means that the broadband absorption of the optical elements in the IOA would need to be tested for higher input powers as well as the thermal management of the enclosure. The latter would be important so that power dissipated into the housing would not misalign the system.

Finally, it is always important to minimize weight for the flight unit. Each mechanical part design will be revised to reduce mass wherever possible while maintaining structural integrity under launch loads. Finally, all mechanical hardware (bolts and washers) will be upgraded from current stainless steel, to certified and traceable National Aerospace Standard grade.

## 3.4 Acquisition, pointing, and tracking unit for fast beam steering

### 3.4.1 Pointing requirements

For any configuration of space or terrestrial links, long-distance QKD will need to be able to point the signal beams accurately from party to party. The task of pointing and tracking objects arises naturally in various fields including astronomy [130] and defense [150]. Since military solutions are out of scope, we investigated common astronomical solutions.

For astrophotography, there are many ways to stabilize and track an image, including an automated telescope mount or a tip-tilt plate/mirror. Both of these methods require some sort of feedback or information on the speed and direction the device should move. Most of these systems are designed to track objects moving at the speed of stars or other astronomical bodies $\approx 0.005^\circ$ /s, and therefore are not necessarily suitable for tracking vehicles or satellites moving at $\approx 1^\circ$ /s. Therefore to achieve the beam pointing task for our long-distance QKD trials, we designed a device similar to adaptive optics devices currently in use for astronomy that will meet our mission requirements.

Before we designed the device we had to first understand how much pointing stability was required. The primary atmospheric effect that influences the beam pointing is turbulence since the beam diameter is sufficiently large from our planned transmitter [124], however it is also affected by diffraction. The pointing error of the entire system included the atmospheric effects, as well as mechanical limitations of encoders and motors and device alignment. The optical losses due to beam diffraction are unavoidable with Gaussian beams, but having an adaptive beam steering system helps to mitigate the effects of turbulence. The basic goal is to have the pointing uncertainty of the system less than the FOV of the receiver so that as much light as possible can be collected. However, it is also advantageous to reduce the FOV of the receiver since this can cut down on noise from other light sources. A selection of FOV appropriate for the light pollution found on a particular vehicle type and testing environment, as well as a description of the channel for the link can then determine the pointing accuracy of the system.

It was shown in [151] that a device collecting light from a selected receiver telescope over a range of $\pm 5.2$ mrad would be able to point the output beam to an accuracy of $\pm 20$ µrad. This would allow the receiver unit to maximize the efficiency of light collection where the photon was incident on the collection telescope. The actual values of these numbers depends on many device parameters, including the FOV of the receiver telescope and the original transmitter beam diameter.

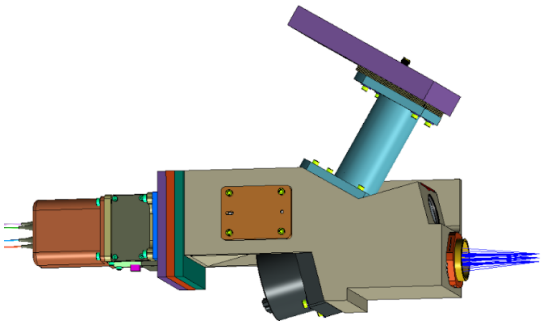
The payload of the proposed QEYSSat mission would incorporate narrow-field quantum receiver optics that will require tracking performance of 20 μrad or better. An APT system will be necessary in order to accomplish the fine pointing of the incoming quantum signal from the collection optics to the polarization analyzers and photon detectors (see Figure 3.1). The desired characteristics of the APT device were as follows:

- "Flight-like" in form, fit and function.
- Interfaces with the QKDR prototype that has been previously demonstrated.
- Have a clear path-to-flight and demonstrate results that can be extrapolated to the QEYSSat mission scenario.

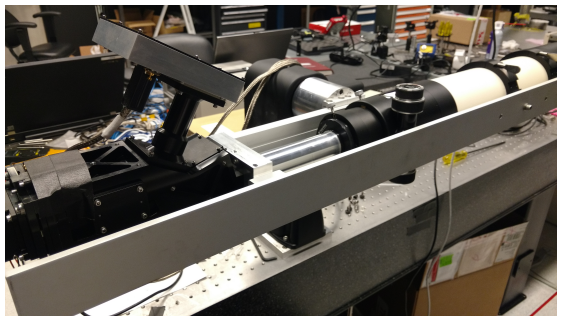
The final design concept for the device is a fast tip-tilt mirror that can steer the beam from the focus of a representative telescope into the entrance pinhole of the IOA. Feedback on the coupling is provided by a beam position on a quad cell detector. The position of the beacon spot (collinear with the signal) on the quad cell is monitored as a function of time. As the position of the beacon beam wanders on this detector, the mirror can move to try and return the beam to a target spot correlated to the optimal transmission for the system.

### 3.4.2 Unit integration and validation

Similar to the development of the IOA, the APT unit was designed in collaboration with industry partners, constructed by the partners, and integrated and tested by our group. A drawing of the APT unit can be found in Figure 3.15a and a photo of the final integrated system in Figure 3.15b. The testing and demonstration procedure was separated into four phases. An initial Phase 0 of basic measurements, such as mass and volume, was performed prior to integration. Phase 1 of the testing and demonstration measured the transmission through the complete system, the stability of the APT pointing, and the polarization effect of the APT mirror over its full range of motion. Phase 2 measured the polarization effect of the APT mirror over its full range of motion while performing QKD. Finally, Phase 3 of the testing and demonstration measured the pointing accuracy of the APT system under angular motion of the telescope with slow and fast fluctuations of the beacon power while also performing QKD.



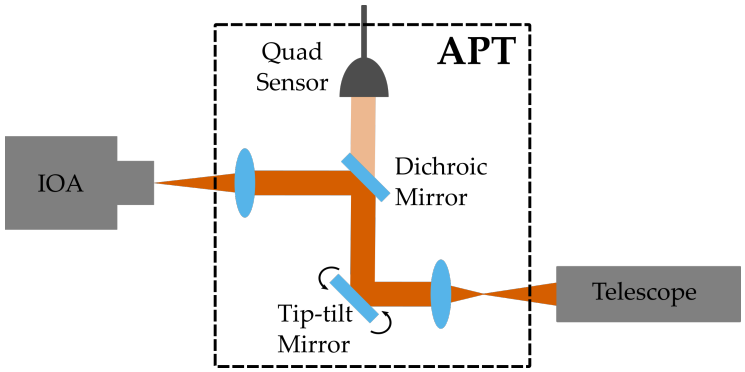
(a) Computer model of the APT unit. Light enters on the right from the focus of a representative telescope and is steered into the IOA in orange on the left side. Computer assisted modeling done by Institut national d'optique (INO).



(b) Photo of the final integrated APT unit with the representative telescope and IOA unit.

Figure 3.15: Acquisition Pointing and Tracking (APT) device schematic, and as mounted for testing. See Figure 3.16 for an internal schematic.

Figure 3.16: Conceptual layout for the internal function of the APT. The tip-tilt mirror stears the beam from the telescope into the IOA with feedback from the quad sensor. The quad sensor uses the beacon beam (at 850nm) picked off at the dichroic to provide feedback for the stearing.




The APT unit needed to be interfaced to two main components, the IOA and the representative telescope. Both physical interfaces needed to be very precisely aligned as the

optical axis for each component must be collinear. The tolerances for the APT/telescope connection were given by analysis from INO: ±0.1 mm for centering of the optical axes, ±10 µm focus location, and ±0.0167° tilt angle between the respective optical axes. For the APT/IOA interface the focus had to be ±10µm. The interface between the APT and the IOA unit was done by INO, by precisely engineering locations for positioning pins and spacing plates to ensure good optical coupling.

In order to make an adapter for interfacing with the telescope, an aluminum mounting bracket was machined in a fashion to the IOA\APT interface. It has two locater pins to align the optical axis, and four screws to connect to the APT unit. To attach to the telescope, it has a female T-thread bore concentric with the opening to the APT unit. This was the most convenient connection point from the telescope focuser assembly to the APT. There is a custom length focuser tube extension between the plate and the stock focuser assembly to put the unit at the right distance from the focus of the telescope. A drawing of the plate and how it connects is shown in Figure 3.15b.

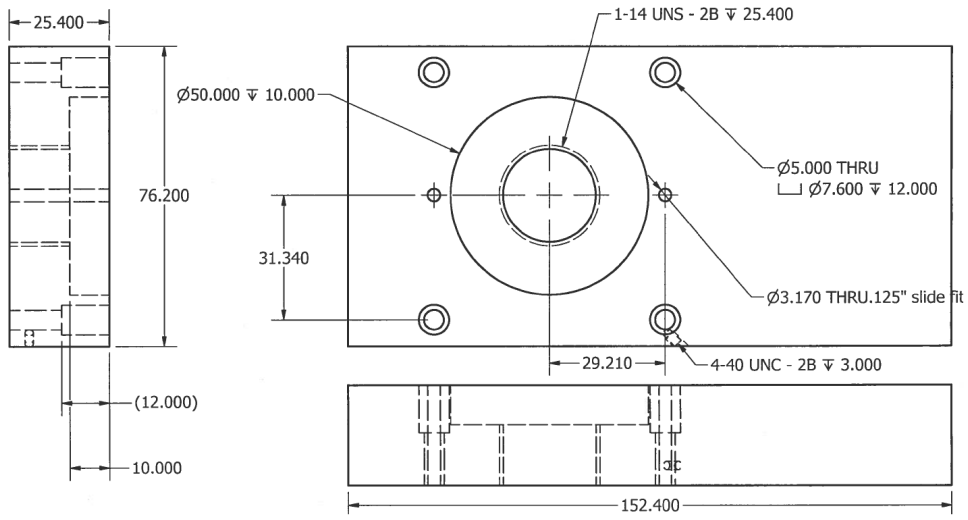



Figure 3.17: Computer assisted drawing of the adapter plate machined to connect the APT unit to the representative telescope. One side of the plate had threads to screw onto an extension tube for the telescope focuser, and the other side had locater pins and threads for interfacing with the APT.

For added stability, two rails were added parallel to the length of the telescope tube that the adapter plate from the APT to the telescope slides on. The slides can be locked to prevent sliding, and the rails add rigidity while the system is in motion. Having the

sliders allows for the finely geared focuser to move the telescope focus in the APT unit manually for alignment. The same rails also facilitate the mounting to the FLIR Motion Control System (FLIR) pan-tilt unit that was used to move the system while testing. Due to also having locking sliders on the FLIR mount, the weight balance on the motors could be adjusted to reduce torque. The FLIR unit was then screwed securely to a large optical table. Photos of the setup are in Figure 3.15b.

### 3.4.3 Basic functionality and initial tracking demonstration

The APT system mass was measured using a scale and found to be 7.13 kg, of which 2.74 kg was from the beacon detector and receiver assembly and 4.39 kg was from the control electronics (3.62 kg from the box and 0.77 kg from the cables). The system volume, measured with a ruler, was found to be 33 cm × 24 cm × 9.5 cm for the optical unit and 33 cm × 24 cm × 8 cm for the control box. An adapter plate was designed and manufactured to mount the APT system (Figure 3.17) to the representative telescope (TeleVue NP101is). For testing the system, a beacon laser with wavelength of 850 nm (measured using a spectrometer) was utilized.

Light tightness was tested by using a flashlight and illuminating various parts of the APT while measuring the output of the IOA on single-photon detectors. The IOA and fibers were covered under a black cloth as the fibers are not light-tight. A suppression of 150 dB was measured. A photo of the flashlight illuminating the APT during the test is shown in Figure 3.18, with the single photon detector counts also shown. Finally, basic behavior of the APT system was determined by sending a beacon signal into the APT unit. The beacon was clearly visible on the provided GUI software and the tracking was functional. The system was found to return to its center position when the beacon was blocked. The mechanism was not able to detect its current position (which was a goal per [APTB-G-101] from [152]).

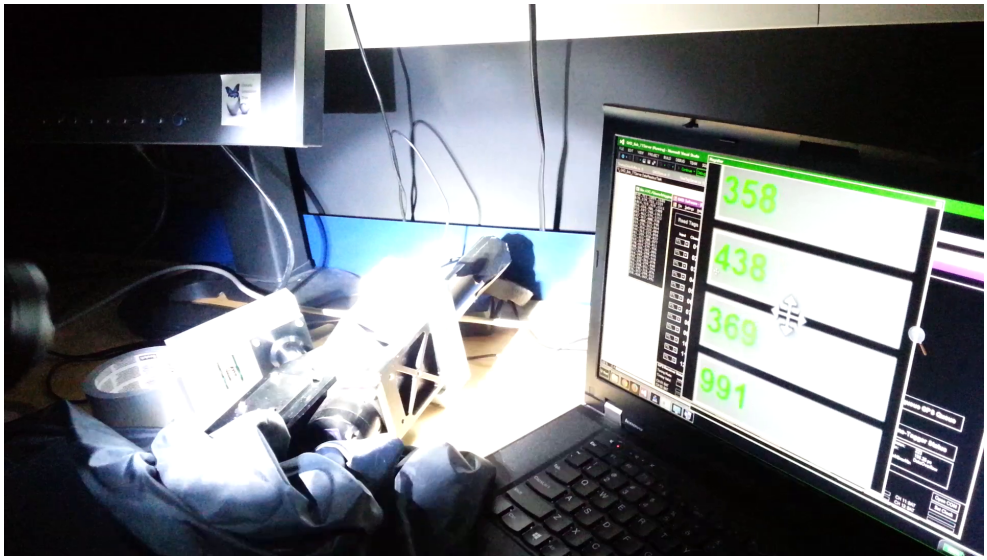



Figure 3.18: Light tightness test setup. The total increase in single photon counts was several hundred to a few thousand, which corresponds to less than 1 fW of optical power.

### 3.4.4 Initial optical characterization

Objectives for this phase:

- Measure transmission and FOV.
- Characterize the polarization effects of the pointing mirror over its range.
- Measure the stability of APT pointing.

Phase one testing was performed with the APT system mounted on the receiver telescope as shown in Figure 3.15b. A 785 nm laser was combined with the beacon laser using a fiber combiner (thereby ensuring collinearity) and both lasers were sent to the transmitter telescope and then to the receiver. With the fine pointing system active, light transmission was measured at the output of the IOA using a power meter to determine the transmission efficiency of the system. The transmission of light at other wavelengths was also measured, using single-photon detectors at the output of the IOA, to determine the filter suppression (see the APT test and demonstration plan [153]).

**Transmission and FOV**

The FOV of the APT system was tested by measuring the 785 nm signal at the output of the IOA (using a power meter) and moving the coarse pointing motor system (with the APT system active) in one direction for each axis until signal was lost. The APT was verified to have a known center position both by blocking the beacon signal and manually interrupting voltage to the APT system and observing the resultant behavior. Polarization characterization was performed by placing a linear polarizer at the input transmitter and adjusting a set of wave plates to adjust the polarization of the 785 nm laser to each of six inputs: horizontal (H), vertical (V), diagonal (D), anti-diagonal (A), right-circular (R) and left-circular (L). The transmission of each polarization was measured at each output of the IOA using a power meter.

Transmission through the APT of the 785 nm laser was measured and found to be 89.7%, after factoring out the transmission losses from the filters and IOA, well above the required 80%. The 850nm beacon transmission was below the noise level of the detectors, measuring a decrease of 18 counts/s with 1.6 μW ($6.8 \times 10^{12}$ photons/s) at the entrance of the APT, compared to the single photon counts measured with the beacon laser turned off. This decrease is within the natural expected Poissonian dark count rate fluctuation and shows a beacon suppression of $> 120$ dB. A count rate increase of 566720 counts/s was measured at 532 nm with a power of 24.8 μW ($6.7 * 10^{13}$ photons/s), giving a suppression of 80 dB. At 662 nm, 760 μW ($2.54 \times 10^{15}$ photons/s) yielded an increase of 333262 counts/s, corresponding to a suppression of 98 dB. All measured suppressions are above the requirements (at least 120 dB for the beacon, and at least 60 dB for other wavelengths).

The field of view of the APT was measured to be $\sim \pm 0.65^\circ$ in the horizontal axis and $\sim \pm 0.55^\circ$ in the vertical axis. The APT system was also verified to return to its center position when the beacon is lost or when the voltage to the mirror is interrupted.

**Polarization effects**

With the APT system active for various coarse motor positions (corresponding to different mirror positions), the intensities at the IOA fiber outputs (corresponding to measured polarizations) were recorded for each of the six input polarization states. The transmissions of the four linear input polarization states used for QKD (H, V, D, A) to the corresponding and orthogonal IOA port are shown in Figure 3.19 and Figure 3.20, respectively. Due to the fact the transmitter is rotated 90° relative to the receiver, the four linear polarizations will also be rotated and each linear polarization at the transmitter will correspond to the orthogonal polarization at the receiver. As such, the expected result of the APT preserved polarization would be 0% transmission in the same IOA polarization port as the input and 50% transmission in the orthogonal polarization port, both limited by the extinction

ratio of the polarizing beam splitters. The orthogonal port only expects 50% transmission instead of 100% because of the non-polarizing beam splitter which splits 50% of the signal to the other basis.

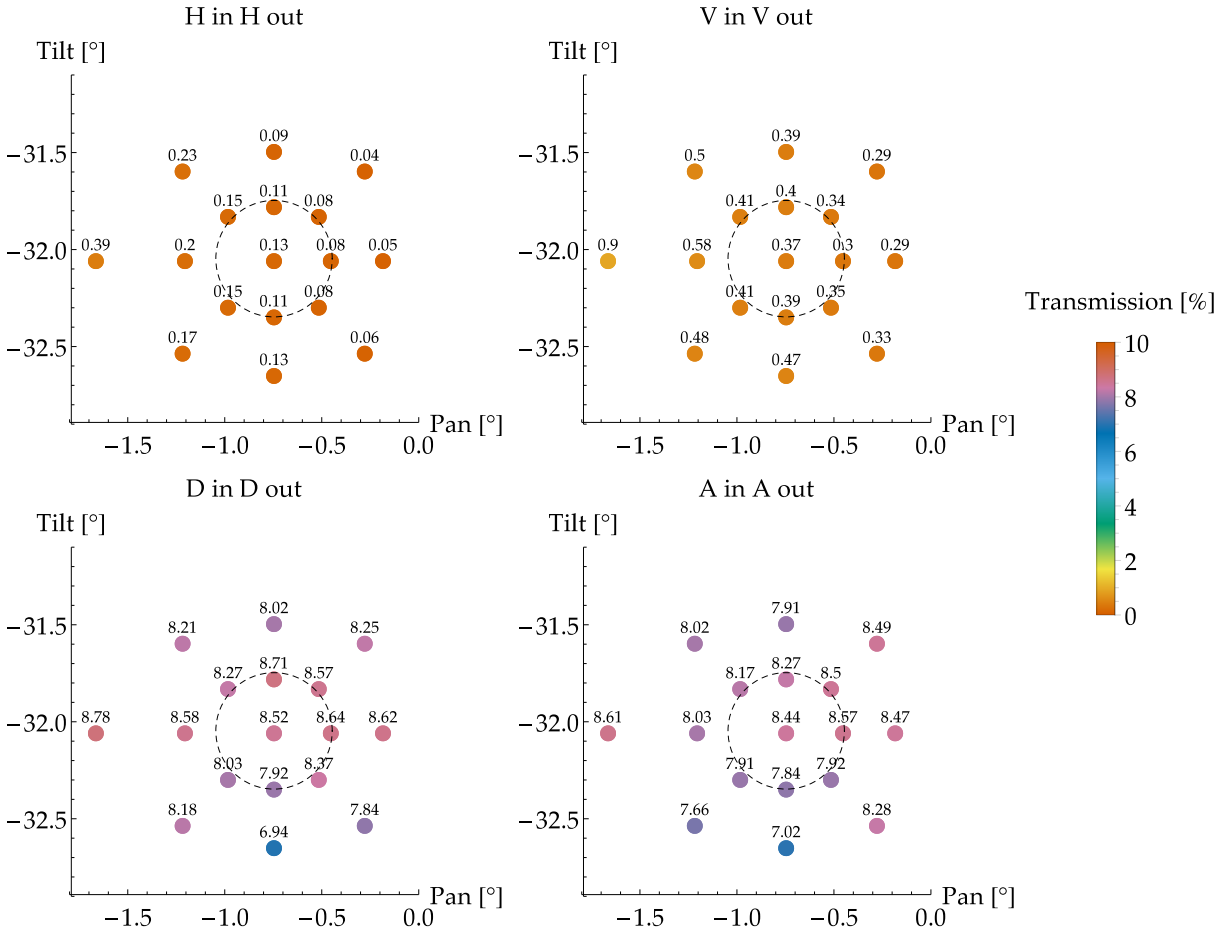



Figure 3.19: Polarization transmission from IOA port with same polarization as input. The expected transmission (assuming no polarization effects in the APT) is a transmission of 0% due to the physical rotation of the transmitter relative to the IOA. While the H and V measurements are close to this expected transmission, the D and A measurement are significantly higher, showing that the APT system imparts a phase between the H and V polarizations. The transmission does not vary greatly across positions, and the variation is mostly due to measurement uncertainty, suggesting the phase is constant. The pan and tilt angles have an arbitrary origin. The dashed circle represents the ±0.3° requirement.

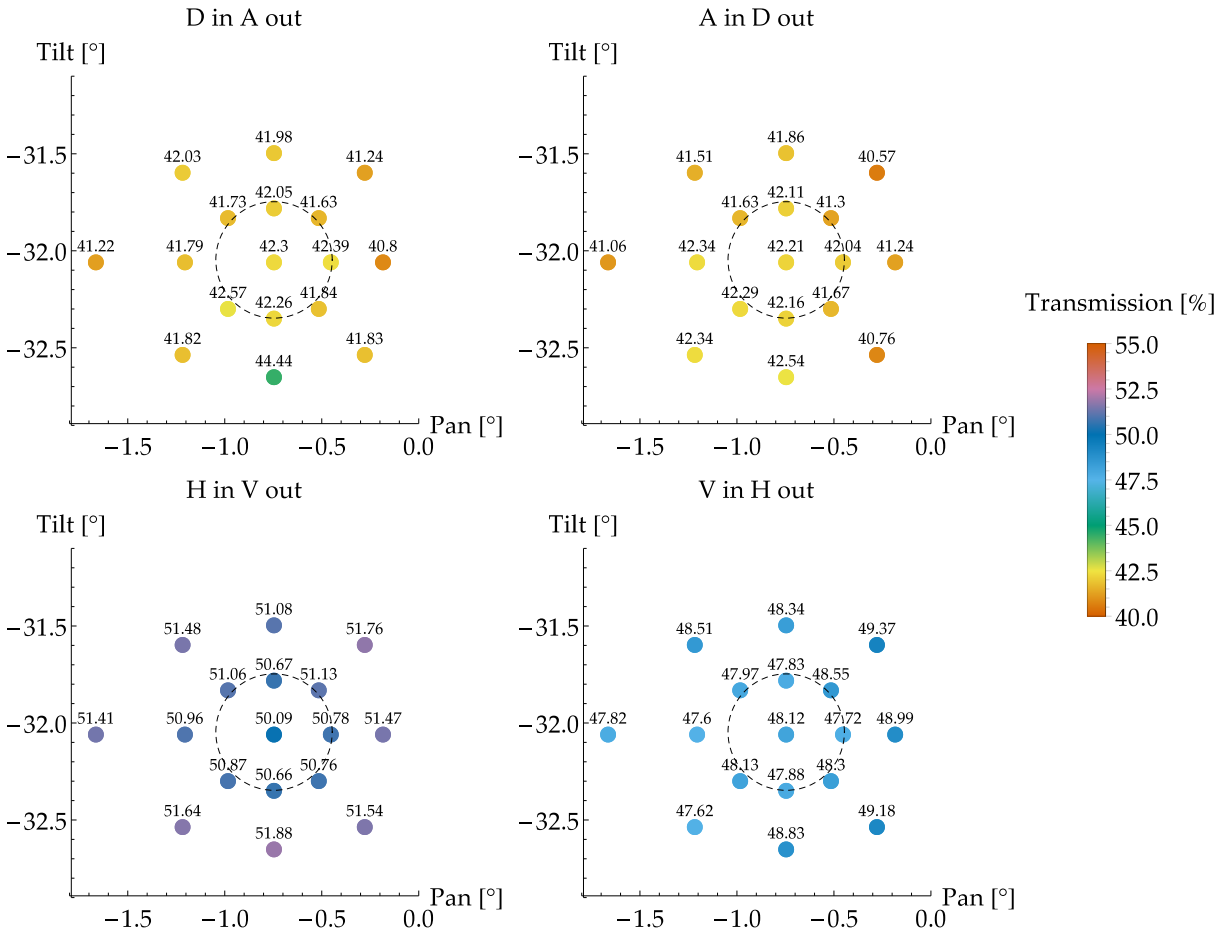



Figure 3.20: Polarization transmission from IOA port with orthogonal polarization to input. The expected transmission (assuming no polarization effects in the APT) is due to the physical rotation of the transmitter relative to the IOA. While the H and V measurements are close to this expected transmission, the D and A measurement are significantly lower, showing that the APT system imparts a phase between the H and V polarizations. The transmission does not vary greatly across positions, and the variation is due to measurement uncertainty, suggesting the phase is constant. The pan and tilt angles have an arbitrary origin. The dashed circle represents the $\pm 0.3°$ requirement.

The results show that the APT system does not preserve polarization, but the change is similar in all positions, suggesting it can be compensated for by imposing a constant phase offset. Alternatively, adjustments to optical components are expected to make this

compensation unnecessary (see APT detailed design final report [132]). The largest transmission variation is 3.6%, which is within measurement uncertainty. The polarization transmission measurements at the center position were used to calculate the compensation required, which was implemented at the transmitter in Phase 2.

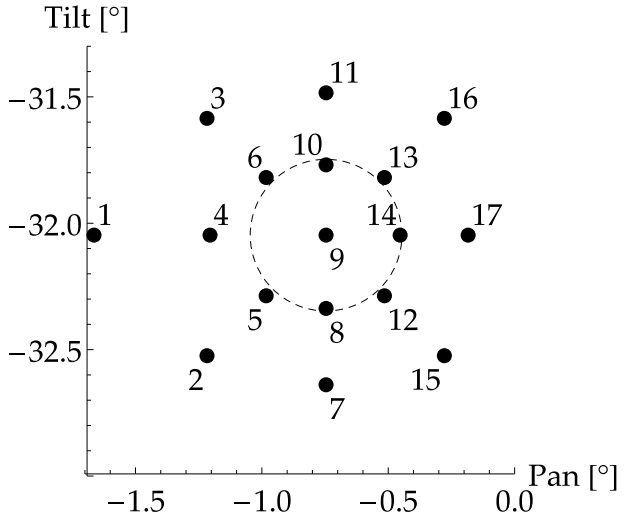
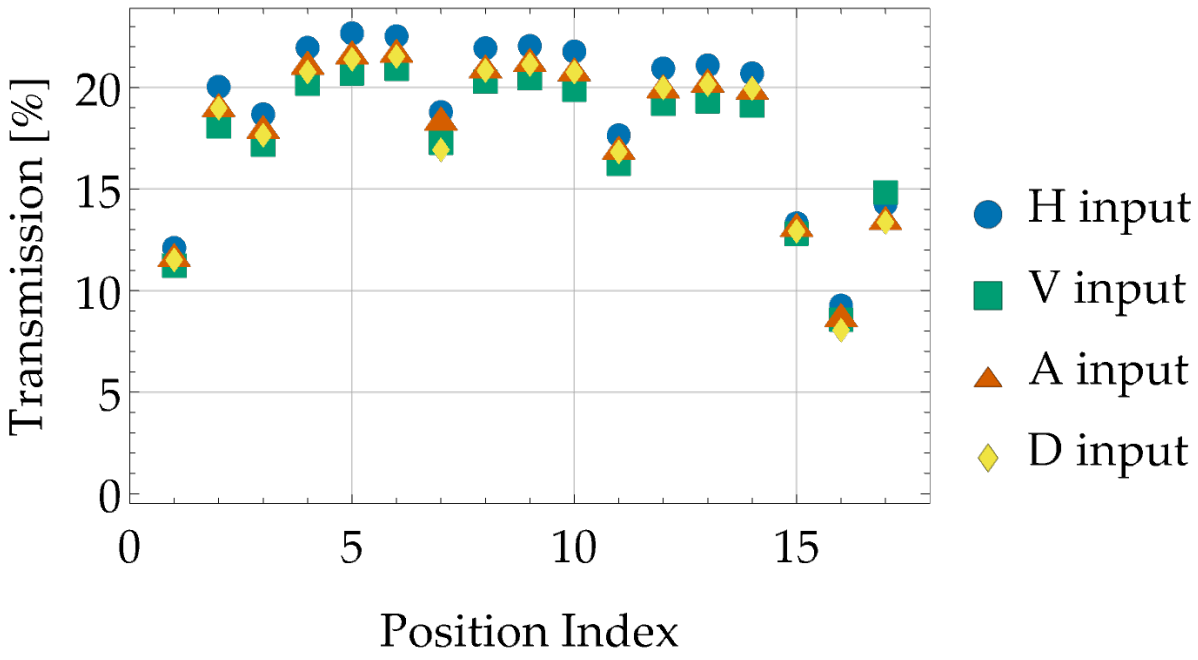



Figure 3.21: Position indices of the Phase 2 Tests. The dashed circle represents the ±0.3° requirement.

The polarization transmission measurement was also used to verify the change in total transmission of the unit with positions. This transmission is shown in Figure 3.22 using the position indices of Figure 3.21. The positions near or inside the ±0.3° requirement maintain an almost constant transmission for all positions, while the positions at the edge show a drop of transmission.

Figure 3.22: Total transmission for each input polarization for each mirror position. The positions at the edge show a drop of transmission at the edges, but the transmission remains almost constant for all positions near or inside the ±0.3° requirement. Note that the transmission is measured from the input of the transmitter telescope, and includes losses in the free-space channel, both telescopes, the APT and the IOA.




**Pointing stability**

Further tests were performed to verify that the drop in transmission at the edges was not due to a variation in the collinearity between the beacon and signal (due to chromatic effects when changing the angle of incidence). For various pan and tilt angles (center and edges in each directions ±0.7° from center), the quad sensor offset was varied. Since the offset position is directly correlated to the signal beam position at the pinhole, varying the offset also varied the signal coupling efficiency at the IOA. The center and full width half max (FWHM) of the signal coupling efficiency distribution was recorded and compared. In all cases, it was observed that the coupling efficiency remained constant over most of the width, only dropping when near the edge. This is consistent with a focused spot size smaller than the pinhole, for which the input position can be varied for a certain range without affecting the coupling efficiency before the edge of the beam begins to be clipped by the pinhole. Therefore, a drop in coupling efficiency due to varying collinearity would

require a change in the center position that is significant compared to the width (a change in center position equal to half of the width would be required to reduce the coupling efficiency by 50%).

The results are shown in Table 3.6. In all measured cases, the change in center position (compared to the center position at pan = -2.0195, tilt = -3.949) is much less than the width. The average FWHM was measured to be 126 µm (X) by 138 µm (Y), almost five times the largest change in X center (26 µm) and more than six times the largest change in Y center (22 µm). This implies that any deviation would be insufficient to cause a significant reduction in coupling efficiency. The measured drop in efficiency at the edges is therefore caused by beam clipping somewhere other than the pinhole (possibly before the tip-tilt mirror).

Table 3.6: Measured center ($X_C$,$Y_C$) and width ($W_x$,$W_y$) on the quad detector of the coupling efficiency distribution

| Pan | Tilt | $X_C$ | $Y_C$ | $W_x$ | $W_y$ |
|---|---|---|---|---|---|
| -2.0195 | -3.949 | 0 | 0 | 122 | 112 |
| -2.3195 | -3.949 | -26 | -14 | 129 | 160 |
| -1.7195 | -3.949 | 12 | -14 | 117 | 128 |
| -2.0195 | -4.249 | 2 | 1 | 140 | 170 |
| -2.0195 | -3.649 | 7 | -22 | 122 | 120 |

The measurement uncertainty was estimated to be around 20 µm, making it unclear if the measured variations were real or the result of measurement error. The results therefore do not confirm the presence of collinearity variation, but do confirm that this possible variation is insufficient to reduce coupling efficiency. As such, the collinearity requirement of 5 µrad has not currently been verified. However, the maximum deviation in collinearity is confirmed to be almost a factor of three less than the acceptance region of the pinhole, which was measured to be 63 µm (X) by 69 µm (Y).

### 3.4.5 Static QKD sampled over FOV

#### Setup

Phase two testing was performed with the APT system mounted on the receiver telescope as shown in Figure 3.15b. QKD signals (at 785 nm) were combined with the beacon laser using a fiber combiner (thereby ensuring collinearity) and both lasers were sent to

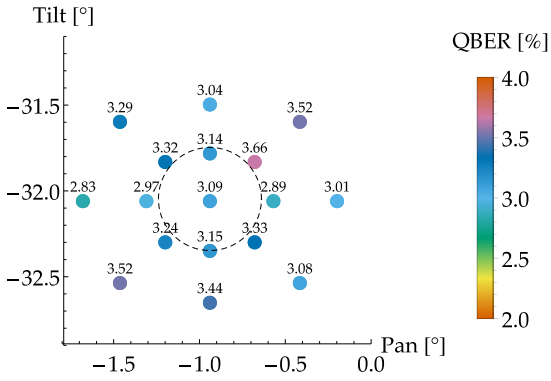
the transmitter telescope and transmitted to the receiver. With the fine pointing system active, transmitted photons were measured at the output of the IOA using single-photon detectors and used to generate a secure key. The polarization effect of the APT system was pre-compensated at the transmitter assuming the effect was independent of the APT mirror position (using polarization measurements from the center position collected in Phase 1). Raw BB84 with decoy states in 100 s intervals were used to generate the ray key that was sifted, and then error corrected with a low-density partity check code [154]. Privacy amplification was performed with Toeplitz-matrix methods [155], and finite-size statistical samples were accounted for [156]. Finally, the generated key is secure as best as pratically can be assured.

### Results

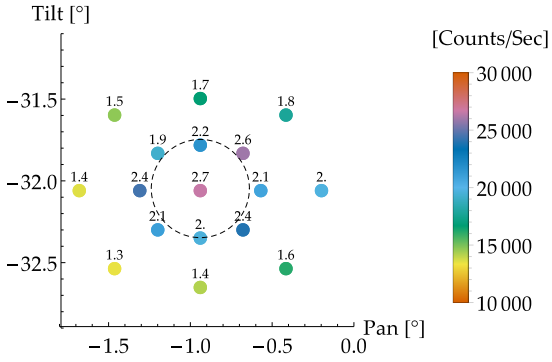
The average quantum bit error rate (QBER) and count rate measured at each coarse motor position (corresponding to various mirror positions) are shown in Figure 3.23a and Figure 3.23b, respectively. While the count rate varied significantly, dropping at the edges, the QBER variation was seen to be small and can be explained by fluctuations in the QKD source (a known property of our apparatus), indicating that the polarization effect of the APT system is constant and can be pre-compensated at the transmitter center.

For each position, 100 seconds of data was accumulated and used to generate secure key including all post-processing steps. The results are shown in Figure 3.23c. Each position was able to generate over 10 kbits of secure key, with a maximum secure key length of 116 kbits. The main cause of the variation in secure key can be seen from the plots in Figure 3.23. Figure 3.24 shows that the secure key length has a strong dependence on count rate, in addition to its dependence on QBER. This large dependence is caused by the strong influence of finite-size statistics in the regime of low total counts (caused by the short duration of 100 s). As a result, the secure key length is highly nonlinear with count rate. Therefore, a 50% drop in count rate can reduce the secure key length to almost zero.

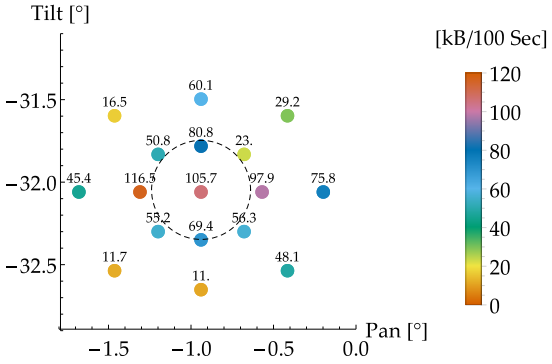
The average loss measured during these tests was $36 - 39$ dB, which was artificially achieved by adding loss between the IOA and detectors to avoid detector saturation. As a comparison, the average total loss predicted for the usable passes in QEYSSat (40 cm receiver), as predicted by the Institute for Quantum Computing (IQC) link analysis, is 42 dB, with the average pass duration being 200 s. The expected loss is a factor of two more than the tested 39 dB and the expected duration is twice the duration tested, so the total counts are expected to be similar. This then leads us to believe we would have similar secure key lengths for this situation.




(a) Average QBER measured at each coarse motor position. The QBER variation can be explained by fluctuations in the QKD source, indicating that the polarization effect of the APT system is constant and can be pre-compensated at the transmitter.




(b) Average count rate measured at each coarse motor position. The count rate dropped significantly at the edges. It was found that the offsets to the quad sensor were not set in the pointing software, which may have contributed to the drop in count rate.




(c) Secure key extracted in 100 s. While the amount of secure key varied significantly, all positions were able to generate over 10 kbits of secure key.

Figure 3.23: Various measured performance parameters of QKD exchange across the APT range.

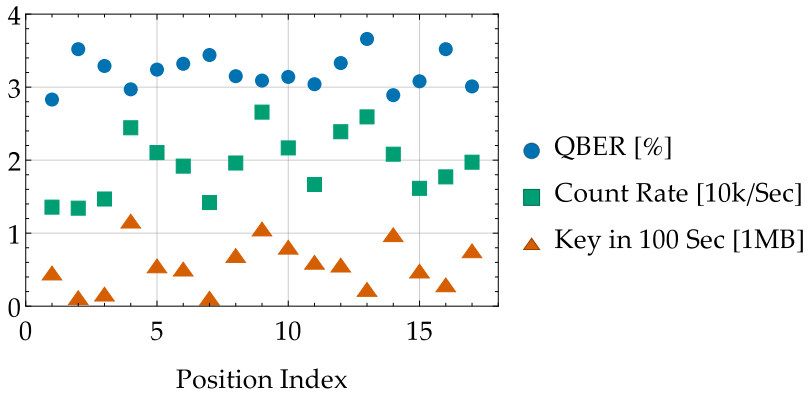



Figure 3.24: QBER, count rate and secure key generated in 100 s. The x axis is just a flattened index of 2-D testing postitions as labeled in Figure 3.21.

### 3.4.6 Pointing and QKD performance

#### Setup

Phase 3 testing was performed with the APT system mounted on the receiver telescope as shown in Figure 3.15b. QKD signals (at 785 nm) were combined with the beacon laser (at 850 nm) using a fiber combiner (thereby ensuring collinearity) and both lasers were sent to the transmitter telescope and transmitted to the receiver. During the tests, the coarse motors were oscillating in one of four pre-set directions: horizontal, vertical, diagonal (where both motors move together in phase) and a circular motion (where both motors move together but with a phase of 90°, drawing a circle around the center position). Two nominal beacon powers were tested, with beacon power modulated around an average value of 50 nW and a maximum value of 7.4 μW (limited by the available power of the laser).

With the fine pointing system active, transmitted photons were measured at the output of the IOA using single photon detectors, and the extractable secure key length was calculated. The polarization effect of the APT system was pre-compensated at the transmitter assuming the effect was independent of the APT mirror position (using polarization measurements from the center position collected in Phase one). Each predicted secure key is based on 100s of data. Due to the fact the motors are not able to generate a pointing oscillation at 20 Hz, pointing data and count rate variation were instead analyzed when performing step movements of 0.05° (greater than the required 0.03°) at a speed of 3.77°/s (corresponding to the maximum speed of sinusoidal motion of 0.03° amplitude at 20 Hz).

### Results

For all four coarse motors motion, QKD signals were collected over 100 s to verify QBER and count rate, and predict the secure key length the system could generate. The motions were performed with an amplitude of 0.3° and a frequency of 1 Hz. This test was performed for a beacon variation of $10 \pm 5$ dB around 2.3 μW (limited by the available power of the beacon laser), a variation of 10 dB around 50 nW and a variation of $20 \pm 10$ dB) around 50 nW. Each modulation was performed at 10 Hz and 100 Hz (sinusoidal modulation).

The beacon power, X error signal from the quad, and Y error signal from the quad were sampled as a function of time at 35Hz. From this data, the mean value and standard deviation are reported in Table 3.7 and Table 3.8 respectively, for each of the various beacon modulation and movement schemes.

Table 3.7: Mean spot error on quad for various movement and beacon fluctuation trials. Many of the trials show a mean very close to 0μm as should be the case. A few of the trials show larger values which can be attributed to a loss in the beacon signal which forces the mirror back to the central position. Once/if the signal is reacquired, the mirror must move back to a pointing position causing larger fluctuations in the errors.

| Beacon power | | 10 μW | 10 μW | 50 nW | 50 nW | 50 nW | 50 nW |
|---|---|---|---|---|---|---|---|
| Beacon power fluctuations | | 10 dB | 10 dB | 10 dB | 10 dB | 20 dB | 20 dB |
| Beacon motion | | 10 Hz | 100 Hz | 10 Hz | 100 Hz | 10 Hz | 100 Hz |
| Vertical Line | X mean | -0.023 | 0.0044 | 0.032 | -0.0057 | 0.3 | 0.045 |
| | Y mean | -0.037 | -0.065 | -0.17 | -0.0056 | 2.02 | 0.021 |
| Horizontal Line | X mean | 0.016 | -0.2 | 0.2 | -0.12 | 1.37 | -0.079 |
| | Y mean | 0.01 | -0.0098 | 0.0059 | 0.015 | -0.11 | -0.031 |
| Diagonal Line | X mean | -0.025 | 0.031 | -0.084 | 0.016 | 0.79 | 0.03 |
| | Y mean | 0.037 | -0.018 | 0.067 | -0.021 | 0.89 | -0.031 |
| Circle | X mean | 0.039 | 0.07 | -0.19 | 0.15 | 2.88 | -0.11 |
| | Y mean | -0.13 | 0.12 | 0.016 | -0.023 | 0.17 | -0.13 |

Table 3.9 and Table 3.10 report the measured QBER and count rates respectively. While the QBER was similar for all tests, the count rate did drop during the test conditions highlighted in the colored table column, but this was found to be largely due to a lower source power during these particular tests. As a comparison, the average count rate measured when the motors where not moving was 36370 counts/s. Table 3.11 shows the predicted secure key after 100 s. As with the count rate, only the tests in yellow showed a

Table 3.8: Spot standard deviation on quad per movement and beacon fluctuation trials. The standard deviation for combinations where one direction is not moving exhibit very low values as should be expected. Trials where there is movement in the particular direction show a range in values. The highest values (which match with the mean data furthest from zero) can once again be attributed to the loss and reacquisition of the beacon signal for a time during the trial.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | Beacon power | 10 μW | 10 μW | 50 nW | 50 nW | 50 nW | 50 nW |
| | Beacon power fluctuations | 10 dB | 10 dB | 10 dB | 10 dB | 20 dB | 20 dB |
| | Beacon motion | 10 Hz | 100 Hz | 10 Hz | 100 Hz | 10 Hz | 100 Hz |
| Vertical Line | X std dev | 3.85 | 3.93 | 3.91 | 3.98 | 9.82 | 4.94 |
| | Y std dev | 22.35 | 22.34 | 22.51 | 22.65 | 51.38 | 22.63 |
| Horizontal Line | X std dev | 25.45 | 25.72 | 25.53 | 25.91 | 66.38 | 25.64 |
| | Y std dev | 1.76 | 2.07 | 1.77 | 1.84 | 16.81 | 1.97 |
| Diagonal Line | X std dev | 18.93 | 18.9 | 18.73 | 18.89 | 37.61 | 18.9 |
| | Y std dev | 14.98 | 14.96 | 14.55 | 14.58 | 30.52 | 14.83 |
| Circle | X std dev | 25.79 | 29.02 | 26.09 | 26.04 | 73.72 | 26.46 |
| | Y std dev | 22.55 | 30.92 | 22.41 | 22.37 | 71.69 | 22.41 |

significant drop, again largely due to the reduced power at the source. All tests predicted a key length above 80 kbits, with only two tests predicting below 100 kbits.

Full QKD protocol post-processing (to extract a secure key) was only performed on one test (circular motion, yellow conditions), which was chosen because it predicted the lowest secure key length of all tests. For the other tests, the secure key length is only calculated and the secure key itself not extracted (by performing the complete post-processing steps). The error correction efficiency (which is the only parameter that can affect the key length in post-processing) is the worst-case error correction efficiency observed in Phase 2 (where the QBER, the main factor affecting the error correction efficiency, was similar or better; the error correction efficiency improves with worsening QBER). The predicted key length is therefore likely to be an underestimate for those tests. The loss during these tests averaged 35 dB, which is less than the loss in Phase 2, allowing both higher count rates and secure key lengths.

### Path-to-Flight Assessment

It was noted that the fine steering mirror actuator used in the current project may not be flight representative. At the component level nothing is currently space-qualified, however,

Table 3.9: Signal QBER measured during tracking tests. The QBER remained fairly constant during all tests, averaging 3.53%.

| Beacon power | 10 μW | 10 μW | 50 nW | 50 nW | 50 nW | 50 nW |
|---|---|---|---|---|---|---|
| Beacon power fluctuations | 10 dB | 10 dB | 10 dB | 10 dB | 20 dB | 20 dB |
| Beacon motion | 10 Hz | 100 Hz | 10 Hz | 100 Hz | 10 Hz | 100 Hz |
| Vertical Line | 3.6 | 3.4 | 3.1 | 3.55 | 3.63 | 3.7 |
| Horizontal Line | 3.87 | 3.36 | 3.29 | 3.52 | 3.65 | 3.69 |
| Diagonal Line | 3.63 | 3.38 | 3.36 | 3.48 | 3.61 | 3.72 |
| Circle | 3.45 | 3.35 | 3.46 | 3.49 | 3.7 | 3.75 |

Table 3.10: Average count rate measured during tracking tests. The count rate remained fairly constant during most tests, averaging 35461 counts/s, very close to the average count rate measured when the motors where not moving (36370 counts/s). Only the 50 nW, 20 dB variation at 10 Hz showed significant change, which was largely due to lower power at the source during this particular test.

| Beacon power | 10 μW | 10 μW | 50 nW | 50 nW | 50 nW | 50 nW |
|---|---|---|---|---|---|---|
| Beacon power fluctuations | 10 dB | 10 dB | 10 dB | 10 dB | 20 dB | 20 dB |
| Beacon motion | 10 Hz | 100 Hz | 10 Hz | 100 Hz | 10 Hz | 100 Hz |
| Vertical Line | 36968.16 | 36750.74 | 36531.17 | 34175.33 | 32780.85 | 36524.24 |
| Horizontal Line | 34892.47 | 38937.97 | 36660.71 | 35430.83 | 28904.82 | 37068.06 |
| Diagonal Line | 36104.38 | 36680.24 | 37771.27 | 36783 | 33497.57 | 37785.05 |
| Circle | 35613.07 | 35254.67 | 35873.58 | 36095.59 | 28779.17 | 34984.54 |

most components have analogs to space components. Path-to-flight for the custom mirrors, narrow band filters and quad cell detectors will also need to be considered.

The APT unit tested we tested was found to be compliant with the required polarization alignment error of less than 4° after polarization compensation at the transmitter. Test reports from INO identified birefringence in the dichroic mirror to be the cause of the polarization error. Our testing confirmed that the nature of the polarization error is birefringence and not depolarization. This is important because birefringence can be compensated for while a depolarization effect cannot.

The polarization error was mitigated by using a polarization compensation system at the transmitter, which was already being used to compensate for birefringence effects in the fibers from the QKD source to the transmitter telescope. This workaround allowed the unit to successfully perform QKD. Results suggest that the remaining polarization error is

Table 3.11: Predicted key length after 100 s during tracking tests. The predicted key length was over 30 kbits for all tests, averaging 142 kbits. Only the 50 nW, 20 dB variation at 10 Hz predicted less than 100 kbits dues to the reduced count rate, which was largely due to lower power at the source during this particular test.

| Beacon power | 10 μW | 10 μW | 50 nW | 50 nW | 50 nW | 50 nW |
|---|---|---|---|---|---|---|
| Beacon power fluctuations | 10 dB | 10 dB | 10 dB | 10 dB | 20 dB | 20 dB |
| Beacon motion | 10 Hz | 100 Hz | 10 Hz | 100 Hz | 10 Hz | 100 Hz |
| Vertical Line | 124600 | 159158 | 149251 | 182253 | 92542 | 118621 |
| Horizontal Line | 103378 | 153139 | 156709 | 175561 | 131570 | 128762 |
| Diagonal Line | 148853 | 136154 | 120576 | 198478 | 151483 | 157327 |
| Circle | 144946 | 187751 | 152924 | 131918 | 89618 | 166659 |

mainly from the QKD source, with the polarization error in the channel being equivalent to less than 4° (0.5% QBER). Therefore, the system is compliant with the requirement [APT-100] when the unit is used with the pre-compensation workaround.

Also, it is important to consider the temperature dependence of the polarization error. An analysis from the dichroic supplier (included in the INO test report [157]) predicted that the new dichroic will incur a birefringence phase variation of up to 0.5° over a temperature change of 40°C. The original dichroic is expected to produce twice the birefringence phase variation (1°). This shows that while the original dichroic performs adequately at room temperature when employing the pre-compensation workaround, it is still expected to incur an increased sensitivity to temperature fluctuation. This increased sensitivity further illustrates the need to employ a suitable dichroic for the expected flight payload, therefore driving the need to maintain the requirement [APT-100] without change.

# Chapter 4

# Investigating physical vulnerabilities in QKD hardware

> Anyways, the key to this plan is the giant laser.
>
> Dr. Evil, *Austin Powers: International Man of Mystery*

## 4.1 Laser damage of components

With our work half done, we now turn our attention to the second step of developing new technology: TESTING. In the previous chapters, we have talked about how to design and build hardware for a satellite receiver, and what are preferable long-distance testing modalities. The need to test the system and ensure that the attack surface is minimized is of utmost importance since this is cryptographic hardware. Since the long distance systems we have been considering so far are not yet robust enough for hacking attempts, we now turn our attention to a commercial, fiber-based Quantum Key Distribution (QKD) system. In this chapter we look at how to use novel attack strategy to break the security of a commercially available, phase-encoded, fiber QKD system.

The inspiration for the attack described here was a side effect observed from a previous attack method [158]. It was found that when trying to control detectors in QKD systems, prolonged exposure to the controlling laser light actually improved the performance of the detectors. The control laser light in [158] was tested over a wide range of powers $0 - 3$ W

and exposed for 60 s sometimes with 900 s ramps up and down from the peak power. The sensitivity improvement was observed in silicon single photon avalanche photodiode (SPAD), but was also tested and observed in superconducting detectors [159].

There are still other types of detectors used in QKD systems, mainly used to monitor for vulnerabilities to other know attacks. As was discussed in chapter 1, the mean photon number for many QKD schemes is a security critical parameter [160, 33, 124, 161, 162, 163]. Other quantum communication protocols also rely on mean photon number for security [164, 165]. Most implemented protocols then have some way of measuring mean photon number before the encoded state leaves the device. If these sorts of monitoring schemes could be targeted and somehow manipulated, then there exist previously known attacks that could be used to eavesdrop on the key exchange.

Though in general, an eavesdropper would not like to improve the characteristics of the devices of her opponents, there is an important observation here: An external party can manipulate components internal to the device without damaging other components. This is the key concept for the attack and why the possibility to successfully implement this attack had been mostly dismissed by the community. *There is no way blindly shooting watts of power into a QKD device can sill leave it functional!* In the context of cryptography hardware, it does not matter how crazy or counterintuitive the attack is. As long as there is even a chance that it could work, the system is not secure. We demonstrated that chance.

In summary: We are interested in trying to find out if there is a way that we can convince Alice that she is sending out pulses with energy below a secure threshold, but really have the pulses contain extra photons that can be split off and therefore compromise the security of the protocol[166, 167].

**Contributions**

I designed and performed the successful damage experiment as well as damage threshold testing of individual components. I also electrically tested dead components after to characterize the damage. Theory for analysis was done with S. Sajeed and V. Makaraov. This work was performed in the lab of Vadim Makarov. Publications resulting from work related or in this chapter: [168, 169, 170]

### 4.1.1 Fiber fuse

If we are going to inject increasing laser power into an optical system, then the ways in which the devices can fail should be noted. In optical fiber systems one of the main effects of increased optical power densities is called fiber fusing. This effect is well documented and

studied [171], and is a pervasive problem in optical fiber components. The phenomenon results from energy densities in glass reaching a critical threshold and then starting a plasma fire in the fiber that propagates back towards the source at $\sim$ 1 m/s. It is this observable propagation back towards the source that resembles explosive fuses that inspires the name. The core of the fiber is catastrophically damaged as the plasma leaves behind a trail of cavities which destroy the transmission of the waveguide (see Figure 4.1). The effect is often caused by improperly cleaned fiber connectors, fibers bent or broken, or material defects in the fiber itself. For standard telecommunication fiber, most components are only rated to work up to 300 mW[172] before there is a risk of fusing the fiber.

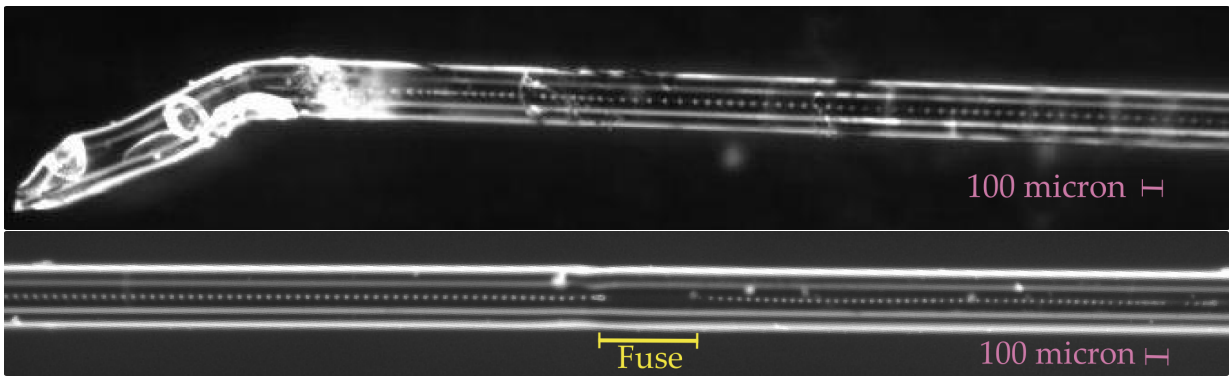



Figure 4.1: Microscope photos of bare telecommunication fiber that was catastrophically damaged from a fiber fuse. The second image shows the fuse propagating through a fusion splice between segments of fiber. The damage stops in the fuse because the core size due to the fusion is slightly bigger than the rest of the single mode (SM) fiber so the critical damage threshold is not reached. Once spatially the mode is better confined, the damage continues.

After describing this effect, it may seem hopeless to cause damage to a component without triggering a fuse. We could certainly inject a large amount of optical power into a QKD device and fuse the fiber, but this would provide no benefit to the eavesdropper and is equivalent to a denial of service attack (cutting the fiber between Alice and Bob). It's similar to taking a sledgehammer to tap in a penny nail, but nonetheless, we wanted to try it and see what would happen. In order to do this in the most responsible way and not wantonly destroy a $\$150,000$ QKD system, we started by testing copies of individual components in the system to see what their real damage thresholds were.

## 4.2 Component testing

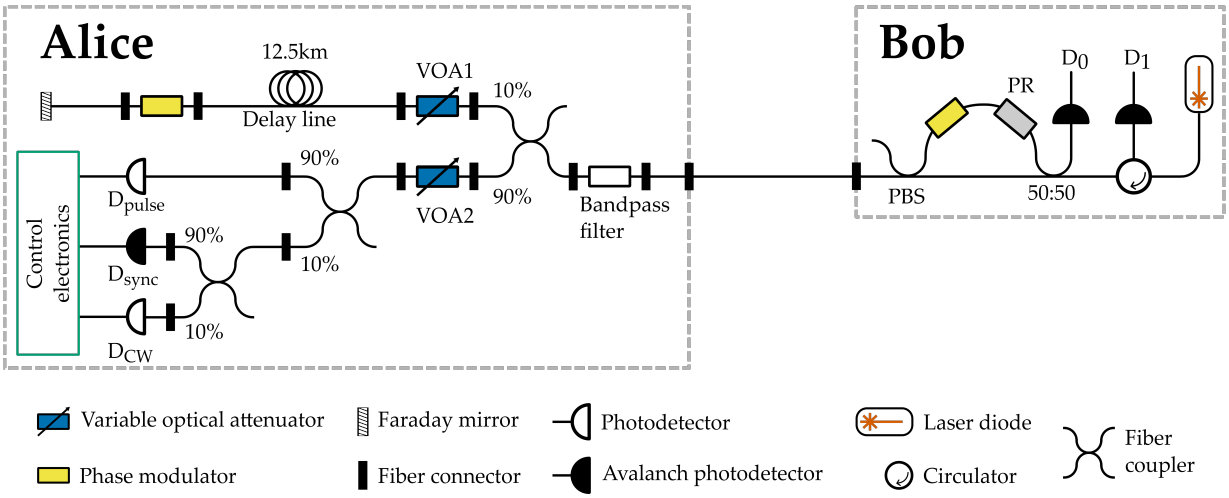



Figure 4.2: The research version of the commercial plug and play QKD (PnPQKD) system tested [160]. The two parties, Alice and Bob, have separate enclosures and are connected by a fiber. In the lab a variable optical attenuator was used to simulate loss from links of more than 1 km.

If we look at Figure 4.7, it presents the schematic for the PnPQKD Clavis$^2$ device. We will discuss how this system works in the next section but what is important to point out here is the types of devices that we need to test the damage threshold on. Alice's device is doing the state encoding so the mean photon number monitoring detectors that we are looking for are located in the bottom half of her setup. For laser light to get from the entrance of Alice's device to these detectors, it has to interact with the following components:

- fiber connectors.
- fiber splitters.
- bandpass filter.
- variable attenuator.
- PIN photodiode $D_{pulse}$ and $D_{CW}$ (JDSU EPM 605LL).
- InGaAs avalanche photodiode (APD) $D_{sync}$ (FRM5W232BS).

Obviously there will be 10% of the injected light directed by the splitter to VOA1 and the bit encoding arm of the device. However, this is a relatively small portion of the injected light and is much harder to replicate the included components and driving electronics. Our approach was to first do all the testing on individual components external to Clavis[2] and then in situ for the detector electronics to make sure the idea was sound to start with. We start by testing copies of the passive components separately, with the assumption that since we are also testing the connectors that there should be no additional potential for damage when they are combined. Then we test the PIN diodes externally by exposing them to a variety of optical power levels for different time periods. This allows us to determine what illumination modes would make the most sense for useful damage in the full QKD system.

### 4.2.1 Passive components

The first components we looked at were the 90:10 fiber splitters. Since they were a very common part, it was easy to obtain many copies and then see how much power they could handle. The testing setup that we used can be seen in Figure 4.4. For all the passive components we test here we use a 70 W, continuous wave (CW) 1550 nm laser provided by Raman Kashyap at École Polytechnique de Montréal. To isolate any damaging effect we saw with the components from that of the connectors, we tested the samples by cutting the connectors off and splicing them directly onto the fiber that the laser was coupled to.

It is a challenge in itself to get 70 W of optical power focused into a bare fiber end. Figure 4.3 shows a picture of the coupling setup. The commercial laser system was fiber coupled out to an attached collimator that created a beam of about 1 cm diameter in free space. We then used two mirrors and a microscope objective to align and focus this beam onto then end of the fiber directly. A glass slide was used as a pickoff in free space beam when not directly testing the components to verify the laser power. In the best case we were able to couple 30 W into bare fiber, but did not have this coupling efficiency when testing components.

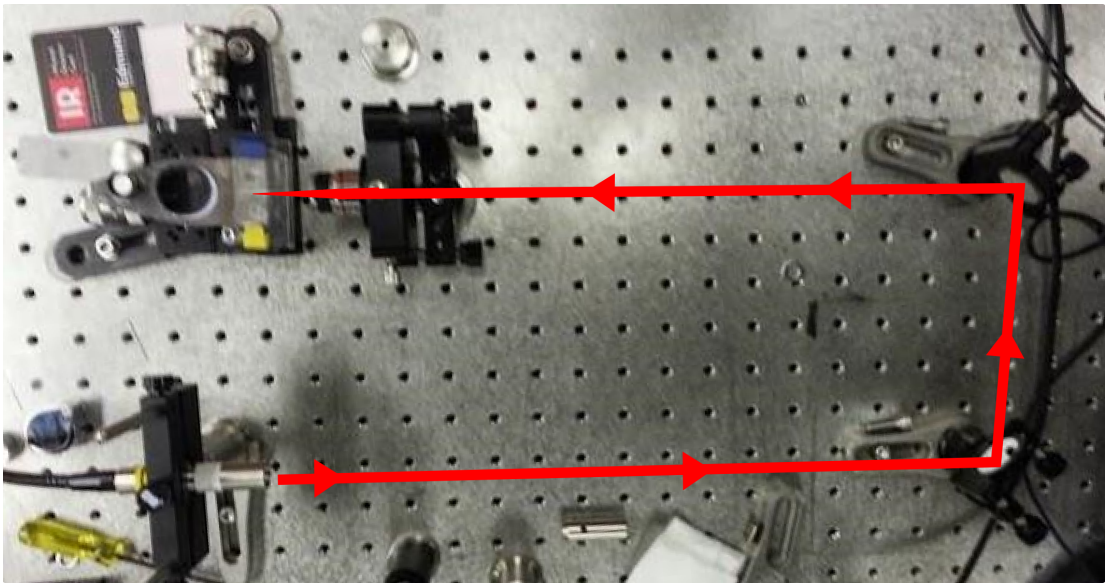


Figure 4.3: High power, free-space fiber coupling set up. The free-space propagating beam was focused with a microscope objective onto the end of a bare fiber which was a few meters of fiber was directly spliced to the component being tested to avoid fusing starting at a coupler.

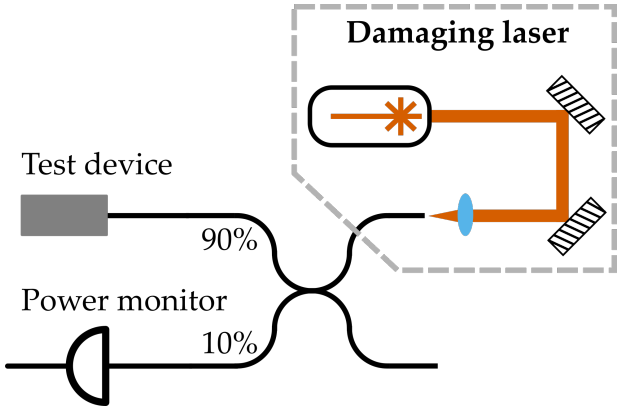



Figure 4.4: Setup used to test the individual fiber optic components for damage threshold. Components were spliced onto a section of bare 1550 nm SM fiber, and their throughput monitored by additional power meters.

All of the cases of testing the splitter resulted in manual ignition of a damaging effect.

The results of the passive component testing can be seen in Table 4.1. With up to 8 W in the splitter and an exposure time $\geq$ 30 min, no damage occurred. There were slight shifts in the splitting ratio after the power had warmed up the device, but after cooling it returned to the original splitting ratio as the change was not permanent. We monitored this by using two power meters to monitor the insertion loss of the splitter and the splitting ratio. You can see videos of the damage that we then initiated for fun here [173].

The variable attenuators used in Clavis$^2$ are very similar models to those used in the lab for just basic testing and they survived as much power as we could subject them to. They have a simple design, the fiber channel converts to a free space beam internally and a finely calibrated stepper motor moves a post or disk to block a portion of the light coupling back into the fiber. These blocks are often made of ceramic so they can handle a lot of power especially because the free space power densities will be lower than the ones in fiber. Given that these components were much more expensive to purchase spares, and the fact that we had used these with high laser power in other contexts we assumed the ones in the device would be fine.

The filter was the last component to splice on and test. Since this is right at the entrance of Alice's device, it will receive the most power of any component. We had one spare of this narrow bandwidth (1 nm) fiber filter, as they had gone out of production. We were hence a bit more cautious with our testing and did not intentionally try and break the component. A power meter was used at the output of the filter to monitor the loss in the device as the power was ramped up. In these tests the power was ramped up to 0.8 W in band, and though the device was warm, it was able to transmit the power for $\sim$ 15 min without any damage.

Table 4.1: Results of select components tested with the setup in Figure 4.4

| Component | Test conditions | Result |
|---|---|---|
| 90/10 fiber coupler | Continuous up to 3W in fiber | fiber fused before coupler |
| 90/10 fiber coupler | Continuous up to 3W in fiber | fiber fused before coupler (magnet) |
| 90/10 fiber coupler | Continuous up to 3.3W in fiber | fiber fused before coupler |
| 90/10 fiber coupler | Maxed out laser at 8W in fiber | no fuse, manually started |
| Narrow-band fiber filter | Continuous up to 800 mW in band | hot, but no apparent damage |

The remaining obvious thing to test was what the damage thresholds were for the FC/PC or APC connectors that were between almost every component in Alice's device. While working on the free space coupling of the 70 W laser, a properly cleaned connector

was spliced on and connected to another fiber with a standard bulkhead. This connector experienced up to 20 W of power and nothing happened, nor when it was swapped to other spare connectors that we had around when the power was off. With all of damage thresholds for the passive components established sufficiently high given what we know damages detectors, we then moved on to testing the PIN diodes.

### 4.2.2 PIN diodes

After verifying the range of powers that we could expect to use with the passive components, next was to look at the PIN photodiodes that are the target of damage. As compared to just testing the transmission characteristics of the passive components there was a lot more to monitor for the diodes. The testing setup was as shown in Figure 4.5. Table 4.2 shows the results of the testing as well as the different damage illumination modes tested. Most of the illumination modes involve exposing the diode to a certain power for a given time and then when the damaging power was turned off, the diode would be characterized.

This characterization was achieved by using a fixed, much lower power characterization laser as shown in Figure 4.5. Light of a known power was applied to the diode and the voltage drop and current across the diode were measured. After this laser was turned off, the multimeter that was used to measure the voltage and current was also used to measure the diode drop in both directions, as well as the resistance across the diode. These latter measures assisted in determining when the diode was about to completely fail and when it did, what was the final electrical state of the diode. After a full characterization of the diode state, the power was increased by a roughly constant increment for that test and the damaging and characterization cycle would repeat until the device failed or a desired state was achieved.

The selection of the illumination modes was motivated by what we saw in the first couple tests as well as limited by the number of copies of the fiber pigtailed PIN diodes we could obtain. This means the diodes were repeatedly exposed and their failure did not necessarily represent the damage done by the final shot in the ramp. Tests 4 and 5 were single shot to address this concern, but obviously much more could be done in this vein to determine even more accurately the paths to optimal damage with lowest power. Since our goal here is security motivated, any possible attack regardless of optimality is a vulnerability so we just wanted to find damage situations that worked.

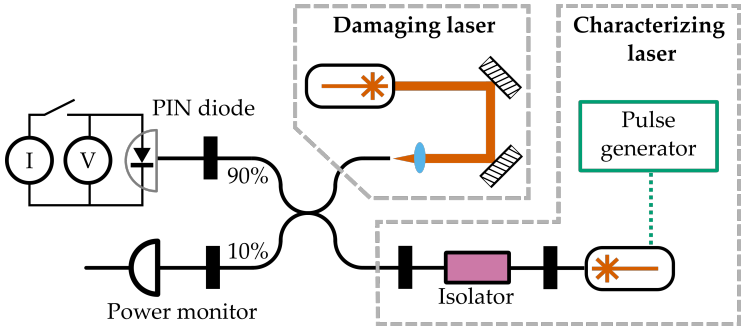



Figure 4.5: Setup used to test the PIN diodes externally.

Table 4.2: Results for testing the PIN diodes in isolation. Diodes were exposed to various illumination patterns to assert which would cause the most favorable results for in situ testing.

| Test # | Test power | Exposure | Result |
|---|---|---|---|
| 1 | Ramped to $\sim 3.5$ W | $\sim 20$ s each | Reduced photosensitivity<br>Open circuit |
| 2 | Ramped to $\sim 5$ W | 3 s each shuttered | Reduced photosensitivity<br>Closed circuit |
| 3 | Ramped to $\sim 0.7$ W | 300 s shuttered | Reduced photosensitivity |
| 4 | $\sim 0.5$ W | 20 s shuttered single shot | Reduced photosensitivity |
| 5 | $< 1$ mW average<br>(1.3 µm, 1 ns pulsed) | 20 s | No change |

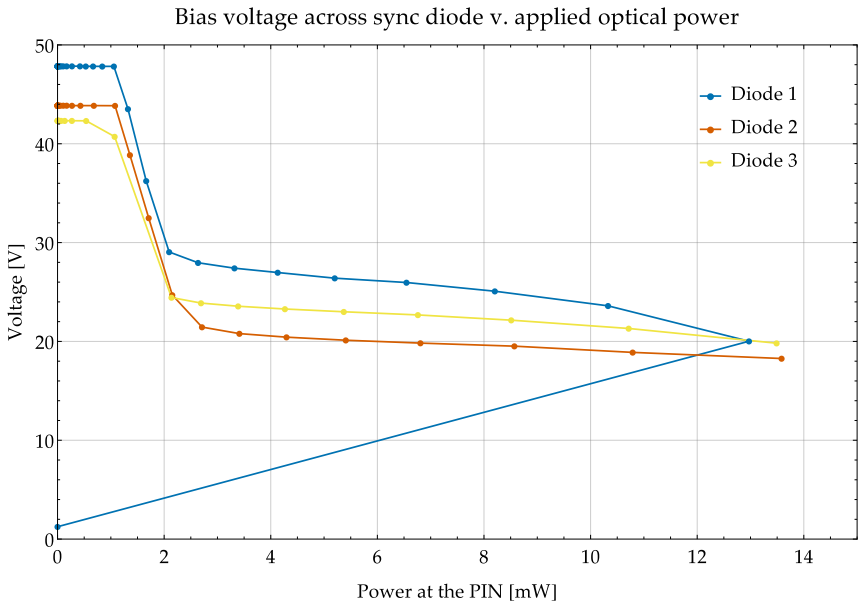
### 4.2.3 Sync diodes

The sync detector ($D_{sync}$ ) is critical to the functionality of the QKD protocol, as is synchronizes the phase modulator with when the pulses stored in the delay line will arrive for encoding. While there are attacks on synchronization of devices [174], this is not the intent here. It is an imperative for this attack that this detector remain undamaged. The supporting electronics for $D_{sync}$ are more complicated since the APD needs to be reverse biased.

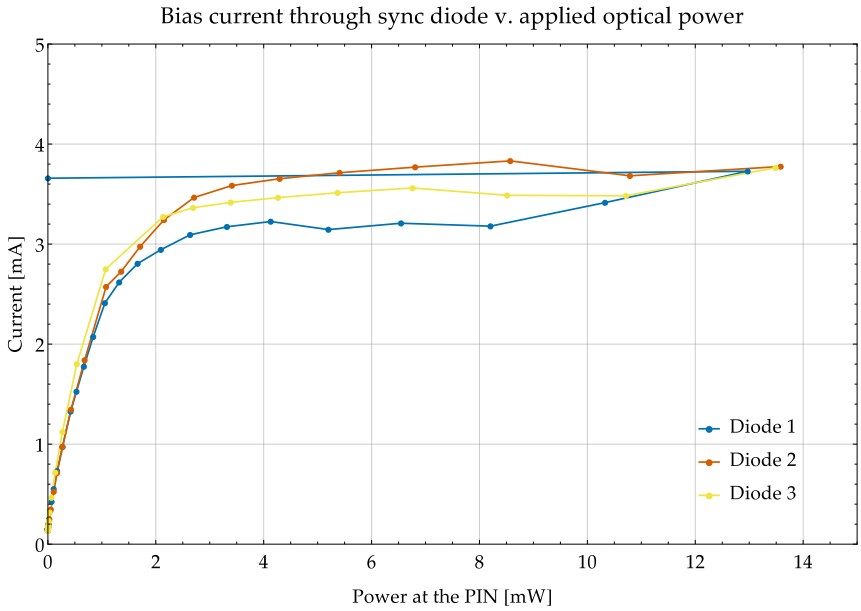
Three copies of the $D_{sync}$ were tested in situ, as they were soldered into the printed circuit board (PCB) inside the Clavis$^2$ device. It was important to the function of the

device that the readout electronics were the same as those in Clavis[2] . It was far easier to replace burnt electronic components than reproduce the circuit. Optically the damaging setup is the same as the PIN diodes, but the characterizing was done all the time to make sure we could catch when the diode died. The monitored parameters were the bias voltage across and the current through the APD.

Of the three tested samples, all of the devices survived illumination levels equivalent to the desired attack powers on the PIN diodes. When the testing was complete on the first diode, the damage illumination was shuttered and the diode shorted closed. From the manufacturer specifications the diode should only be exposed to $\sim 400$ μW. By looking at the biasing circuit in Clavis[2] , we can see if the voltage drop across the diode drops suddenly there are charged capacitors that will dump their current across the diode. This is speculated to be the damage mechanism, but not knowing the specifics inside the diode, it is not easily verified. With the subsequent diodes, we verified if the damaging illumination is slowly ($\sim 5$ s) ramped up and back down at the end, there is no damage and it returns to normal operation. The bias voltage and current through the diodes under damaging illumination can be seen in Figure 4.6.




(a)




(b)

Figure 4.6: Plots of the bias voltage on the APD and the current through the diode as a function of the illumination power. The first diode shorted, resulting in a very low bias voltage for the device.

## 4.3 Live attack on commercial QKD system

After we were satisfied with the results from the individual component testing, the next step was to try this on Clavis$^2$ while operational. By applying $0.12 - 2$ W of in-band, CW laser power into the fiber optic channel, we controllably destroyed security critical components inside the sender Alice. The pulse energy monitoring photodiode ($D_{pulse}$ ) lost photosensitivity, which left the system operational but permanently insecure. Damage was performed on a running system without interrupting key distribution.

### 4.3.1 Plug and Play scheme

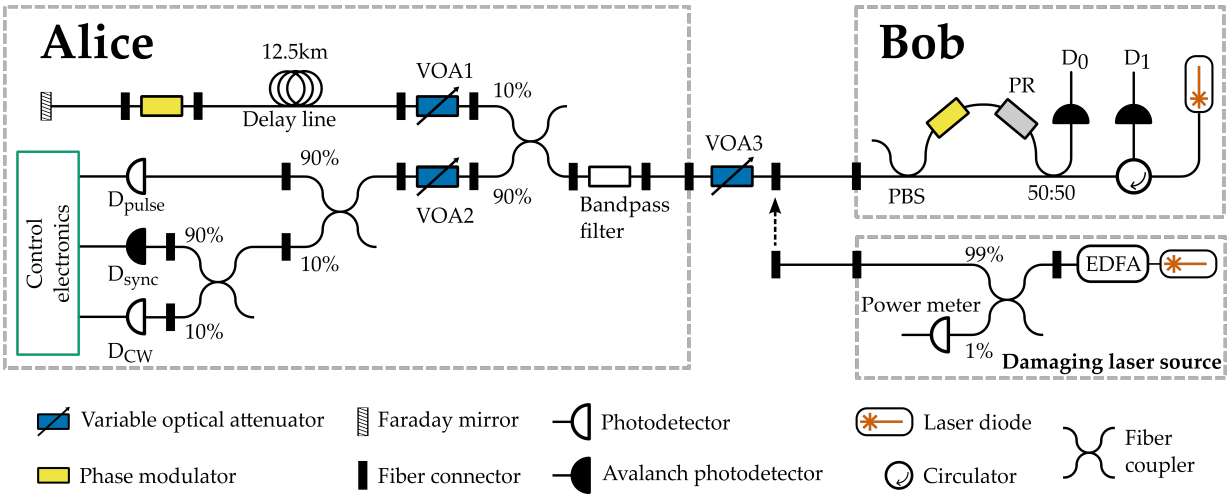



Figure 4.7: The research version of the commercial PnPQKD system tested. The two parties, Alice and Bob, have separate enclosures and are connected by a fiber with a variable optical attenuator which simulated loss from a longer link.

Here one commercial QKD system was tested, but this technique could be adapted to potentially any system with energy monitoring detectors. Here we use a research version of the commercial Clavis$^2$ QKD system. Clavis$^2$ is a fiber based, PnPQKD commercial QKD system that uses phase-encoded information on weak coherent pulse (WCP) to send the key bits[160]. The basic scheme for the system can be found in Figure 4.7.

Alice and Bob use a standard BB84 protocol[20], and are connected by a optical channel for transmitting the photons, and a classical channel to facilitate necessary classical

communication for the protocol. To avoid the difficulty of actively correcting for the birefringence of the optical channel, the laser source is located in Bob and pulses are reflected back at Alice and attenuated so that the pulses then travel both directions through the fiber. Bob sends bright (mW) pulses that get polarization and time multiplexed by his unbalanced interferometer. For each laser pulse, there is two sub-pulses that travel to Alice and back that will be recombined when they go though Bob's unbalanced interferometer again. Scattering effects of strong pulses from Bob interacting with weak reflected pulses from Alice would increase error rate of this system so Bob sends his pulses in groups of about 1700 called frames, and Alice has a delay line that is used to store the incoming pulses so that all the strong pulses are in the delay before the modulated pulses are reflected back.

The pulses are sent through the optical channel and Alice has the task of measuring the incoming power of pulses so that she knows how much to attenuate them. Alice can calculate the required attenuation based the desired security parameters. After the pulse is reflected she uses her phase modulator to modulate the phase of one of the sub-pulses with one of four states $(0, \frac{\pi}{2}, \pi, \frac{3\pi}{2})$, two each in two different bases. This modulation is only applied to one of the two sub-pulses per laser pulse so that when they are recombined in Bob, the bit value can be read out based on the interference between the modulated and unmodulated sub-pulses. Bob then detects the interference with his two single photon detectors and records all the outcomes. Then so that Alice and Bob can share the same error free key, they use classical communication channels to perform standard key sifting, error correction, and privacy amplification steps of a Bennett-Brassard 1984 (BB84) protocol.

$D_{pulse}$ is a standard PIN photodiode that has electronics which integrate over the time bin for each pulse to try and calculate the energy contained in each pair of sub-pulses. It receives the most light of the three detectors, $\approx 81\%$ of the incident light at Alice. In this system, this integrated value is only monitored when in crosses a calibrated threshold, but no alert is given for too little light. This will be valuable for the attack as it will not raise any alert when the detector is damaged. For more information on the subsequent electronics, see [169].

$D_{sync}$ receives $\approx 8.1\%$ of the incident light and is a high bandwidth APD that is in charge of edge detecting incoming pulses to coordinate Alice's phase modulator. The last detector $D_{CW}$ is a PIN that receives $\approx 0.009\%$ of the incident light and is designed to monitor the average incoming energy so as to detect if extra light is being injected. Proper use of this detector in the system is not fully implemented as we are using a research version of the commercial system.

To ensure proper calibration of the system and specifically the detector electronic

thresholds, each device is tested at the manufacturer. This process is mainly responsible for the setting of the alert threshold on the pulse energy monitoring detector. $D_{pulse}$ monitors only whether the integrated optical energy exceeds an electronic threshold, called an alert. At the manufacturer, the system is set up and runs a special software package that one can monitor the triggered alerts in the system. Normally, alerts are not reported and if the number of alerts in a frame is above a certain number per frame, the data for the entire frame is just thrown out. The proper level for this detector is calibrated by using the fixed operational power of the laser in Bob and known optical channel losses. Then the threshold is set so that there are no alerts and the smallest decrease of the threshold generates alerts. This ensures the highest sensitivity of this threshold. It will tolerate up to a 10% fluctuation in alerts per frame before it throws out the data for the frame. The system then makes a function fitting the tested line losses and stores the parameters in the device firmware for all future uses of the system. This process is done once when the device is assembled, and will not be revisited unless the system is sent back for maintenance.

### 4.3.2 QKD operational sequence

When this commercial system is installed, all one does is connect the network and the optical fiber and it will calibrate and calculate all necessary operational parameters. In this research version we had access to, the system asks for some of these parameters at the start of operation so that it can proceed to the key exchange more quickly. When our system is turned on it first spends a few minutes cooling down the detectors and lasers in Bob, and then checks the dark count levels in the detectors in Bob. Next it configures the gate timing for the detectors relative to the laser pulses in Bob. The user then provides an estimate of the optical line length and the uncertainty of that value. The system then scans the gate timing on the detectors to maximize the counts with the laser just constantly pulsing. Then both Alice and Bob set their phase modulator to all the setting combinations to check that the visibility of the detections that Bob registers are correct according to the settings. Lastly, the user tells the system whether to run BB84 or SARG protocols for QKD and then starts the raw key exchange. For these experiments we always chose BB84. Then the systems exchange raw key until one of two end conditions: either the internal memory buffer for recording the detections is full, or one of the parameters it monitors throughout the exchange drifts out of predefined boundaries.

Once the system has stopped exchanging key, it moves on to the key distillation step and uses the classical link to sift, error correct, and apply privacy amplification to the raw key. Then depending on why the previous key exchange failed, the system will either return to an appropriate calibration procedure or start another raw key exchange. When

the system decides that it needs to return to calibrate or remeasure a parameter, it can often take a few minutes for it to return to key exchange, especially if it cannot resolve the conflict. This is when the ideal time to attack the system was chosen. The hacker can cause errors in the system and not raise alerts as the system is in the middle of determining what would constitute an error. It is also fairly common that some natural errors will cause a raw key exchange to stop and fail the distillation process. It is these natural errors in the software sequence that eavesdroppercan execute her attack.

### 4.3.3 Hacking setup

To damage the pulse energy monitoring detectors, a coupler and an erbium-doped fiber amplifier (EDFA) were used to inject $0.5-2$ W of optical power into the optical transmission line between Alice and Bob. A diagram of the attack setup can be found in the bottom right of Figure 4.7. The laser diode used to seed the amplifier was tuned to the same wavelength as the lasers in Bob, so that it would pass through the filter at the entrance of Alice. At the current time, the research version of the system has no active feedback from the detectors to the attenuator VOA2, and it is just set at 2 dB before the detector timing calibration starts.

Before each repetition of the attack protocol, the Clavis$^2$ system was started up normally and allowed to generate secret key to ensure the system was operational. The ideal point in the systems' operational sequence was difficult to find, but our best results came when we started the attack at the beginning of a raw key exchange. This then almost guaranteed the system would not get stuck in recalibration procedures and seamlessly generate key post attack. To execute the attack, the optical channel was disconnected from Bob and then Eve's coupler was connected to Alice. The damage was done over a short $\sim 3$ min period with controlled, high power exposure of $20-30$ s depending on the trial. The rest of the attack time was due to the power ramp time of the fiber amplifier and physically connecting fibers. The optical channel was then reconnected, and the system would try to resume key exchange. In about half of the trials, the system recovered on its own, and would resume generating secret key. In the rest, it got stuck in recalibration protocols so it was restarted and then continued to generate key.

The applied power was measured by comparing the power of the 1% pickoff at the exit of the EDFA and the the power at the pigtail of the $D_{pulse}$ detector in Alice that $\sim 40\%$ of the light from the amplifier made it to the desired detector. After it was verified that the system was operational and had completed a few more key generation cycles, the system was stopped. The manufacturer calibration software was then started and then used to characterize the alert level post damaging.

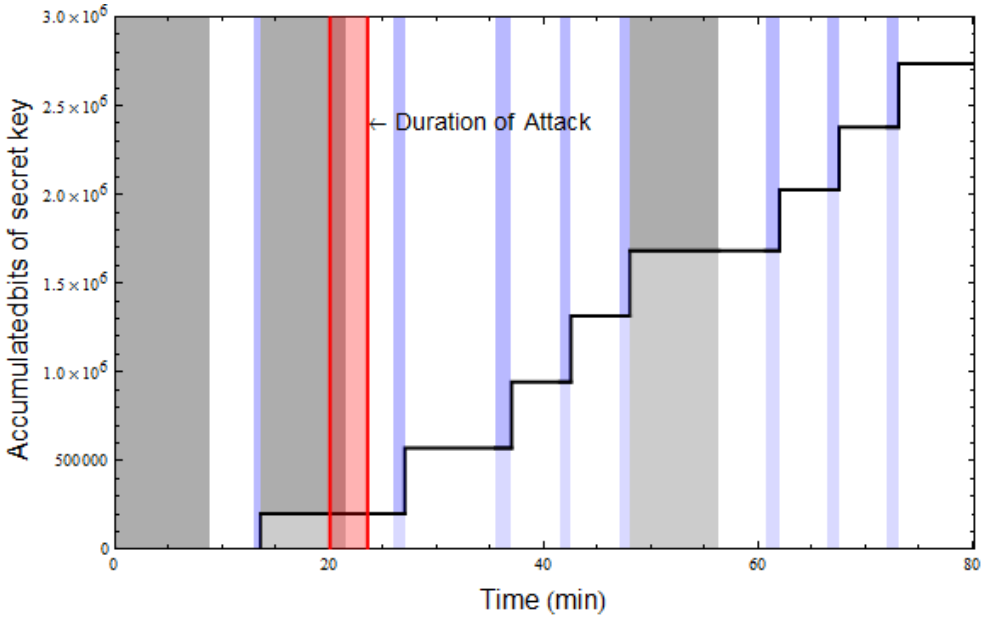



Figure 4.8: Accumulated secret key produced by the system as a function of time. Blue bands indicate the system was distilling key, gray bands the system is recalibrating, and white the system is in raw key exchange protocols.

## 4.4 Results of attack

### 4.4.1 Physical damage to the detectors

After the damaged diodes were electrically characterized and removed from the system, they were physically opened to document the physical damage to the material. Figure 4.9 shows macroscopic demonstration of the damage that occurred in the external PIN testing in test # 2. In Figure 4.10, microscopic images of the detector active areas that were damaged in situ can be seen.

Figure 4.9: Macro photos of the internal structure of the PIN photodiodes. The diode can be seen as the chip on the right post in each picture. The left photo is of an undamaged diode and the one on the right is from external diode test number #2. Photo credit Makarov Lab.

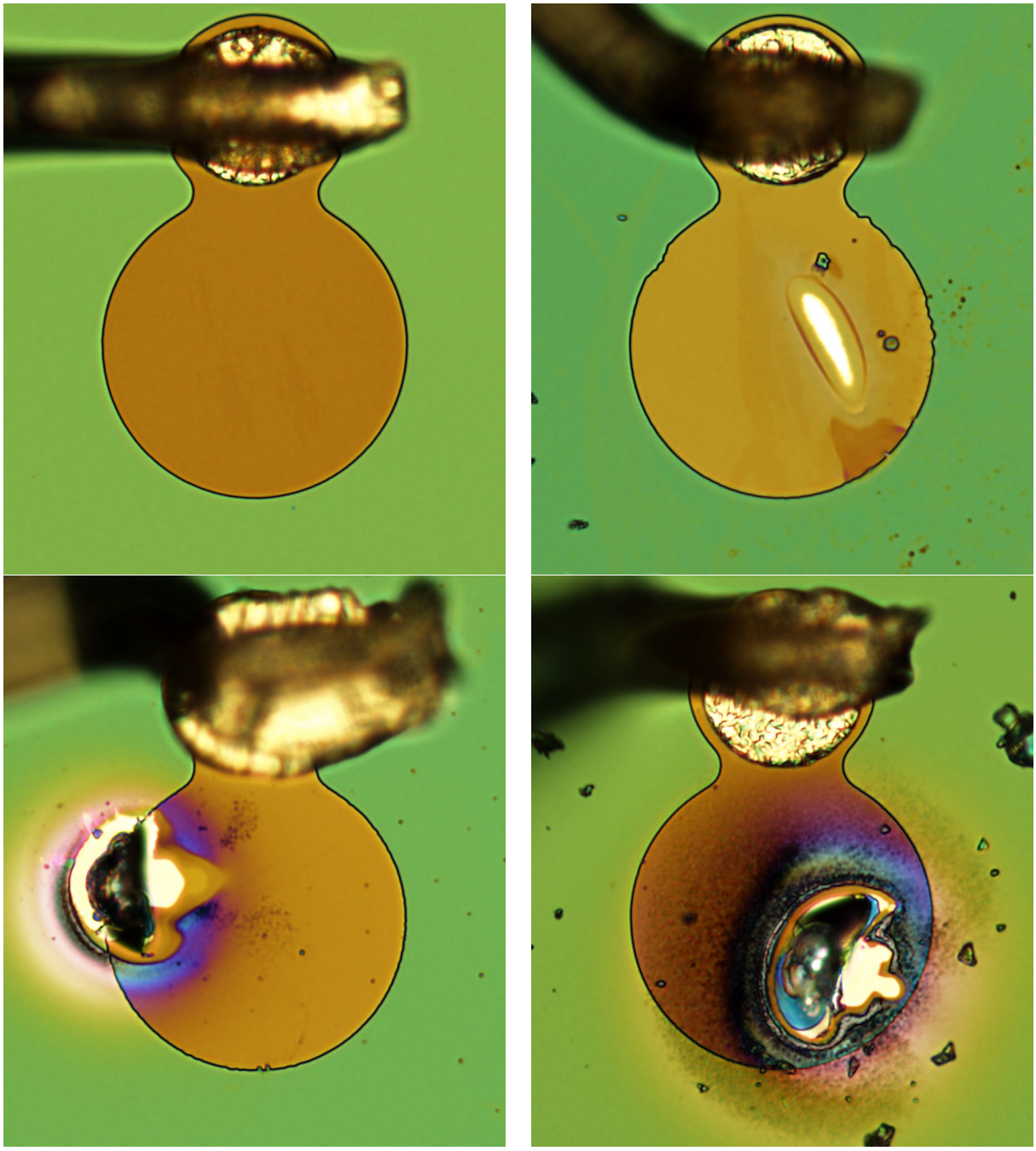


Figure 4.10: Microscope photos of the internal structure of the PIN photodiodes. Top left is an undamaged detector, top right is the diode from in situ test #8, bottom left is from the in situ test #3 and bottom right if from in situ test #6. Photos from [168].

### 4.4.2 Altered parameters

This attack sequence was performed on 8 distinct diodes, with varying attack power and duration. For each trial, a new, identical $D_{pulse}$ was installed and electrically characterized before and after the damage. The results of all the trials can be seen in Table 4.3. In 2 trials, there was procedural errors that resulted in no damage to the diode. In 3 tests, the diodes had 1-6dB of additional light allowed proportional to the applied power. The remaining 3 tests had the most promising results, a complete desensitization of the detector by either burning it to an open circuit or a large resistor where the dark current did not trigger an alert. Figure 4.8 shows the accumulated secret key as a function of time during the system operation. This particular data came from a test where the diode was open circuited to no sensitivity and recovered autonomously after the damage. To the hacker, this would be the ideal outcome for the attack, no detector sensitivity and no system disruption.

Now we have done the tricky part, but now need to actually describe how the hacker gets the secret key bits. This last part of the demonstration was not physically implemented due to time and cost, but is quite easy to simulate. Firstly we have to decide what type of attack that eavesdropper will use given the now demonstrated reduction in sensitivity of $D_{pulse}$ . We will choose as a realistically implementable attack that eavesdropper will use an unambiguous state discrimination (USD) [89] attack with probability $p_{\text{attack}}$ and do nothing with probability $1 - p_{\text{attack}}$.

The security analysis for this attack is similar to that described in [169]. Figure 10 from [169] shows a plot of the fraction of key leaked compared to the multiplication factor of the light allowed by a detector. The mechanism of the reduced sensitivity is different in this proof, but is generally applicable here as the important consequence is the reduced sensitivity of the detectors. Now, if we consider a realistic attack with 0 pulses suppressed (as we are not doing that here) we see that around a multiplication factor of 3, the entirety of the key is leaked to eavesdropper. Looking again at Table 4.3 the minimum sensitivity reduction was 1 dB and maximum was 6 dB (with complete insensitivity being like $\infty$ dB). The tests that did 5 dB $\approx$ 3.2x or more will reveal the entirety of the key to eavesdropper.

### 4.4.3 Conclusion

There are various countermeasures that could be implemented to prevent this type of attack. Optical fuses [175] are in-line fiber components that can catastrophically damage when the power through them is higher than a certain threshold. A device like this at

Table 4.3: Results for the in situ testing of the laser damage attack. The damage conditions and result are listed below for each of the diodes, some diodes were used for multiple damaging exposures.

| Diode # | Damage power (W) | Damage time (sec) | Restart needed? | Result |
|---|---|---|---|---|
| 1 | 0.5 | 20 | Y | Shifted Unity Alert up 1dB, Dark alarm level went up |
| | 0.75 | 20 | Y | Shifted Unity Alert up 6dB, Dark alarm level went up |
| 2 | 1 | 20 | Y | User error, no change |
| 3 | 1 | 20 | N | Shifted Unity Alert up 5dB, Dark alarm level went up |
| | 1.5 | 20 | N | Shifted Unity Alert up 5.5dB into sync saturation range |
| 4 | 1.5 | 30 | N | Shifted 20% Alert into sync saturation range, Dark alarm level went up |
| 5 | 1.7 | 20 | N | No alerts ever, open circuit |
| 6 | 1.7 | 20 | Y | No alerts ever, large resistor |
| 7 | 1.7 | 25 | N | 1-2% alert with no sensitivity |
| 8 | 0.75 | 20 | Y | No change |
| | 1 | 20 | Y | Shifted Unity Alert up 1.6 dB, sharp transition |

the entrance of the system could stop the injected light at the cost of having to have it physically attended to repair the system back to working order. Also, depending on the timescale of the fuse mechanism, the hacker could cause enough damage that would go otherwise unnoticed after the fuse was replaced.

Another option for countering this attack is to use higher speed attenuator at VOA2 with a robust feedback from the pulse energy detector. Again, if the damage was done quickly enough the attenuator may not be able to stop it. An obvious inclusion to the detector itself is having at least two thresholds for the pulse energy so that it can tell if there is no sensitivity or input power. Other electrical parameters of the detector could also be monitored to try to detect damage. However, all of these measures would simply tell the user that they have to come replace damaged components to maintain the security of the system, and do not actually prevent the hacker from attacking and changing things

to start with.

In this study, we have shown that it is possible to use strong laser light to attack a running QKD system. The system was exposed to the light while operating, and would after the exposure ended, would continue generating secret key. After it was shown the system continued to operate normally, factory calibration software was used to characterize how much damage was done to $D_{pulse}$ . This then breaks the security of the QKD system as in most of the trials, enough extra light was injected to allow the hacker to perform a photon number splitting attack and gain up to 100% of the secret key.

# Chapter 5

# Conclusion

Information security is always in flux and should never be treated as something static. The introduction of quantum resources has perturbed the classical status quo and it is our responsibility as a society to make sure that we cryptographic tools to protect our information. Quantum Key Distribution (QKD) is an opportunity for us to leverage this new technology, and there has been many advances so far in the field. However, a proof of principle is not sufficient for the development of commercial technologies, there has to be a cycle of breaking devices and improving them to ensure the quality and security of the hardware. This work has simulated and done preliminary testing for airborne tests of QKD, made improvements and designed new components for QKD hardware, and demonstrated a novel hacking technique on a live commercial QKD system.

In chapter 2, the conditions for testing a QKD device on a moving platform are modeled for both stratospheric balloons and aircraft. There are various advantages and disadvantages to each type of platform, but it was concluded for the vehicle opportunities presented, our payload will be tested on an aircraft. The biggest deciding factors in this were the mission parameters for the balloon launch. With the constraint that the other experiments on the flight wanted to study sunrise and daytime light conditions, it was difficult for us to get enough nighttime testing. Choosing the ground station location for the balloon based on pointing altitude was the most successful method shown, but clearly other hybrid methods could also improve the outcome. In summary, it was shown that a stratospheric balloon test of a QKD receiver would be feasible with more control over the launch.

The aircraft alternative looked at in chapter 2, mitigated much of the risk introduced by a balloon test, but of course had constraints of its own. The specific vehicles that we had access to imposed geometric constraints that were modeled and then optimized

with a useful tool for designing the experimental flights. Preliminary tests were performed with the payload in the Beechcraft Bonanza, and demonstrated that the classical link and surrounding infrastructure were working. This modeling and preliminary testing was important to help address one of the main problems facing larger acceptance of QKD. There is already much activity in the area of laser communication and an excellent opportunity to improve the available security infrastructure.

The next steps for work in this chapter is already in progress, which is using the aircraft modeling tools to facilitate actual airborne tests of the quantum key distribution receiver (QKDR) payload. Doing airborne tests, in addition to additional environmental testing of the hardware are all important steps to take to maximize the viability of the hardware for a satellite. Hopefully once there is enough testing on this system, a satellite like the Quantum Encryption and Science Satellite (QEYSSat) design could be launched and a new regime for quantum communication could be explored. There are also many other interesting fundamental experiments that could utilize a satellite to explore the interactions of relativity and quantum mechanics [176].

Next, in chapter 3 three important components for a space QKD are presented. A detector package was designed and built to be space qualified or have a clear path-to-flight for all included parts. The performance of the device exceeded the requirements specified by link simulations from [125]. The second device was an Integrated Optical Assembly (IOA) which had physical stability suitable for field testing/extreme environments. Thirdly, an adaptive optics unit (Acquisition Pointing and Tracking (APT)) was designed, constructed, and tested to steer photons collected by a telescope into the IOA. All of these components were integrated and are in use for current airborne testing. As was noted with all the components developed in chapter 3, the path-to-flight was identified which are explicit next steps for advancing the QKDR prototype.

Lastly, a novel laser damage attack was performed on a running commercial QKD system. The attack used a slowly ramped, high power, continuous wave (CW) laser to reduce the sensitivity or completely destroy a security critical monitoring detector. All of the relevant components were tested to explore what the damage threshold for the components were. The damage threshold for the PIN diodes was found to be quite low and the psdiode would not be damaged if the power was ramped slowly over seconds. The destruction of this detector allows in over half of the cases for eavesdropperto learn up to the full key so this is a very compromising attack.

The extensions of QKD protocols and hardware are also important to examine. Obviously there are important use cases that really can benefit from the security of QKD, but there are some significant ways in which it is not a complete solution. Post-quantum

cryptography [177] is another critical piece to upgrading our cryptographic infrastructure. Unlike QKD which requires some moderate to major overhauls of optical telecommunication infrastructure, Post-quantum cryptography provides alternate algorithms for cryptographic protocols that can be run on current hardware. A major future direction for both of these fields is to develop hybrid solutions that incorporate QKD for highly sensitive information and seeding the post-quantum algorithms.

# APPENDICES

# Appendix A

# Mathematica code for flight path analysis

Listing A.1: Mathematica code for modeling the optimal flight path to maximize the Quantum Key Distribution (QKD) link time and generate flight conditions similar to that of a satelight overpass. It assumes the geometric constraints for the quantum key distribution receiver (QKDR) payload in a Beechcraft Bonanza and the plane parameters are derived from this vechicle's specification. The target satelight pass conditions are 1°/s and a link of 100s. The physical constraints of the Bonanza are stated in the first five lines of code.

```
αmin = 11.5 °; βmax = 42.5 °;(*Pan Range*)
δmin = 17; ϵmax = 39; (*Tilt range. FLIR is negative, but abs is used here.*)
planespeedmin = 100; planespeedmax = 370.4; planespeedmid = 166.68;(*Speed given in km/h*)
beaconDivergence = 0.32 °;

tiltAngle[d_, x_, h_] := ArcTan[h/Sqrt[d^2 + x^2]]*180/π
linkLength[d_, x_, h_] := Sqrt[d^2 + x^2 + h^2]
x[t_, τ_, d_] := d Tan[αmin] + (t*d Tan[βmax])/τ
r[t_, τ_, d_, h_] := Sqrt[(x[t, τ, d])^2 + d^2 + h^2]

(*Pan*)ϕ[t_, τ_, d_] := 180*ArcTan[x[t, τ, d]/d]/π
(*Tilt*)θ[t_, τ_, d_, h_] := 180*ArcSin[h/r[t, τ, d, h]]/π

dϕ[t_, τ_] := (60.32538595984022` τ)/(
 1.4491603270989837` t^2 + 1.1672380672397038` t τ + 1.` τ^2)
dθ[t_, τ_, d_,
  h_] := -((78.86087504110917` d^2 h (0.554309051452769` + (
```

```
          1.3763819204711734` t)/τ))/(Sqrt[
        1 - h^2/(
         d^2 + h^2 + (0.554309051452769` d + (
            1.3763819204711734` d t)/τ)^2)] (d^2 +
          h^2 + (0.554309051452769` d + (
            1.3763819204711734` d t)/τ)^2)^(3/2) τ))

dϕmax[τ_, d_, h_] := (60.32538595984022` τ)/(
 0.` + 1.` τ^2)
dθmax[τ_, d_, h_] :=
 Maximize[-((78.86087504110917` d^2 h (0.554309051452769` + (
           1.3763819204711734` t)/τ))/(Sqrt[1 - h^2/(
          d^2 + h^2 + (0.554309051452769` d + (1.3763819204711734` d t)/τ)^2)] (d^2 +
           h^2 + (0.554309051452769` d + (1.3763819204711734` d t)/τ)^2)^(3/2) τ)), t][[1]]
dϕθmax[τ_, d_, h_] := \[Sqrt]((dϕmax[τ, d, h])^2 + (dθmax[τ, d, h])^2)

height[ location_GeoPosition ] :=
 QuantityMagnitude[UnitConvert[Quantity[location [[1,  3]], "m"], "km"]]
beaconSpotDia[d_, x_, h_] := (Tan[beaconDivergence]*linkLength[d, x, h]*1000)*2
totalTiltRange[d_, {xmin_, xmax_},
  h_] := ( tiltAngle [d, xmin, h] - tiltAngle[d, xmax, h]) // N

sty = Directive[FontFamily → "Palatino Linotype", Black,
   FontSize → 18, PlotMarkers → {"•"},
   PointSize → .035];
plotopts =
  Sequence[GridLines → Automatic,
   PlotStyle → Directive[Thick, colorsafe [[6]]], Frame → True,
   ImageSize → 600, LabelStyle → sty, AxesStyle → sty];

ClearAll[plotTiltRange]
plotTiltRange[d_, {xmin_, xmax_}, h_, opts : OptionsPattern []] :=
 Plot[ tiltAngle [d, x, h], {x, xmin, xmax},
  opts,
  PlotRange → {{0, 10}, {0, 60}},
  AxesLabel → {"Distance past transmitter [km]",
    " Tilt angle [°]"},
  Epilog → {colorsafe [[7]], Dashed, Thick,
    Line[{{0, ϵmax}, {10, ϵmax}}],
    Line[{{0, δmin}, {10, δmin}}]}(*Tilt range boundries*),
  PlotLabel →
   " Tilt angle [°] v. x [km] with feasable tilt range"]
plotTiltRange[d_, {xmin_, xmax_}, h_, {δmin_, ϵmax_},
  opts : OptionsPattern []] := Plot[ tiltAngle [d, x, h], {x, xmin, xmax},
  opts,
```

```
  PlotRange → {{0, 10}, {0, 60}},
  AxesLabel → {"Distance past transmitter [km]",
    "Tilt angle [°]"},
  Epilog → {colorsafe [[7]], Dashed, Thick,
    Line[{{0, δmin}, {10, δmin}}]}(*Tilt range \
boundries*),
  PlotLabel →
   "Tilt angle [°] v. x [km] with feasable tilt range"]

ClearAll[plotdϕθmax]
plotdϕθmax[τ_, d_, h_, opts : OptionsPattern []] :=
 Plot[\[Sqrt]((dϕ[t, τ])^2 + (dθ[t, τ, d,
       h])^2), {t, 0, τ},
  opts,
  PlotRange → {{0, τ}, {0, 1.5}},
  AxesLabel → {"Time of contact [s]",
    "Total angular speed [°/s]"},
  PlotLabel → "Total angular speed [°/s] v. contact time [s]"]

optimalDisplacement[alt_] := Module[
  {sol = Flatten[
     Solve[
      N[tiltAngle[d, d Tan[βmax // N], alt]] == δmin, d],
      2]},
  If[Length[sol] > 1,
   sol[[2, 2]],
   Message[anglerange::arng]; 0
   ]]
optimalDisplacement[alt_, limit_] := Module[
  {sol = Flatten[
     Solve[N[tiltAngle[d, d Tan[βmax // N], alt]] == limit, d],
     2]},
  If[Length[sol] > 1,
   sol[[2, 2]],
   Message[anglerange::arng]; 0
   ]]
optimalGPSStart[gs_, d_, heading_] :=
 LatitudeLongitude[
  GeoDestination[GeoDestination[gs, {Quantity[d, "km"], heading}],
   GeoDisplacement[{Quantity[d Tan[αmin], "km"],
     heading - 90}]]]
optimalGPSEnd[gs_, d_, heading_] :=
 LatitudeLongitude[
  GeoDestination[GeoDestination[gs, {Quantity[d, "km"], heading}],
   GeoDisplacement[{Quantity[d Tan[βmax], "km"], heading - 90}]]]
```

```
flightPathMap[gs_, d_, heading_] :=
 With[{min = d Tan[αmin], max = d Tan[βmax]},
  With[{minpos =
111       GeoDestination[GeoDestination[gs, {Quantity[d, "km"], heading}],
         GeoDisplacement[{Quantity[min, "km"], heading − 90}]],
      maxpos =
       GeoDestination[GeoDestination[gs, {Quantity[d, "km"], heading}],
        GeoDisplacement[{Quantity[max, "km"], heading − 90}]]},
116    flightPathMap[gs, d, heading, minpos, maxpos]]]
flightPathMap[gs_, d_, heading_, minpos_, maxpos_] := GeoGraphics[{
   GeoMarker@gs(*Center*),
   GeoMarker@
    GeoDestination[
121      gs, {Quantity[d, "km"],
       heading}](*Direction transmitter is looking*),
   GeoCircle[gs, Quantity[d, "km"]],
   GeoPath[{gs, minpos,
     (*GeoDestination[gs,{Quantity[d,"km"],heading}],*)
126      maxpos, gs}
    ]},
  GeoRange → Quantity[10, "km"],
  GeoBackground → "StreetMap",
  ImageSize → 600,
131  ImagePadding → None]
Flatten[Solve[
  N[tiltAngle[d, d Tan[βmax // N], 2]] == δmin, d], 2]
```

# Appendix B

# Python control for single photon detectors

Listing B.1: Functions used by the program that runs the detectors.

```
'''
Helper functions for I2C interfacing
Sarah Kaiser
Created: Mon Feb 3 2015
Last updated: Fri Mar 28 2015

'''
import sys
import math
import array

'''
General Utilites
'''
lsb = 2*2.5/4096;

#Resistance of thermistor as a function of temperature
def Rthermistor10k(temp):
    return 10000*math.exp(3892*((298.15-(temp+273.15))/(298.15*(temp+273.15))))

#Temperature of thermistor as a function of resistance
def Tthermistor10k(R):
    return (326.3457990944156-273.15*math.log(0.0001*R))/(13.053831963776624+math.log(0.0001*
        R))
```

```
#This changes a passed int into the n character hex string representing that number
def int2phex( intval ,n):
            hexval=hex(intval) [2:]. zfill (n).upper()
            return hexval
#This changes a passed int into the 2 character hex string representing that number
def int2phex2( intval ):
            hexval=hex(intval) [2:]. zfill (2).upper()
            return hexval

#This changes a voltage into a codeword
def v2code(v):
            code=int(round((v*4096)/(2.5-lsb)+lsb))
            return code

#switch to 10 bit readout
def hex10bitcode(hex16):
    return int(bin(int(hex16,16)) [2:]. zfill (16) [4:],2)

#convert 10 bit codeword to voltage
def code2volt(code10bit,adcrange):
    return ((adcrange-2*lsb)/(4096))*code10bit+lsb

#read data to a string
def list2string ( list ):
    return "".join(map(int2phex2, list ))


'''
DAC converting functions
'''
# Convert User HV to hex code
def volt2hex(HVval,channel):
    # Check for invalid voltages
    if (HVval > 500) or (HVval < 0):
        print "User error, stupid voltage choice. Does not compute. Please try again."
        code='0000'
        return '0000'
    else:

        if (channel=='1'):
            code=int2phex(max(int(round(7.41129*HVval-10.922907)),0),4)

        elif (channel=='2'):
            code=int2phex(max(int(round(7.3529590*HVval-7.1530270)),0),4)
```

```
            elif (channel=='3'):
                code=int2phex(max(int(round(7.3563918*HVval-9.2322928)),0),4)

            elif (channel=='4'):
                code=int2phex(max(int(round(7.3705900*HVval-5.7497629)),0),4)

            #original test diode code
            #code=int2phex(int(round((6.99655*HVval+4.125)),4)
            return code

    # Convert User temp to hex code
    def temp2hex(temp):
        # Check for invalid temps
        temp=int(temp)
        if (temp > 50) or (temp < -50):
            print "User error, stupid temperature choice. Does not compute. Please try again."
            return '0000'
        else:
            r=Rthermistor10k(temp)
            rdivide=2.5*(r/(r+65000))
            code=int2phex(v2code(rdivide),4)
            return code

    # Convert User comparitor level to hex code
    def comp2hex(comp):
        # Check for invalid voltages
        if (comp > 500) or (comp < 0):
            print "User error, stupid threshold choice. Does not compute. Please try again."
            return '0000'
        else:
            code=int2phex(v2code(comp/211.5),4)
            return code



    '''
    ADC converting functions
    '''
    # Convert User hex code to HV
    def hex2volt(hexval,channel):
        intcode=2*hex10bitcode(hexval)
        if (channel=='1'):
            volt=0.1477883263281572*intcode-0.011304923293643755
```

```
            elif (channel=='2'):
                volt=0.14913241674799574*intcode+0.26857746986763315

        elif (channel=='3'):
            volt=0.14835849676737672*intcode+0.6480556230452933

        elif (channel=='4'):
            volt=0.14865430420790374*intcode-0.408404208038313

        #original detector equation
            #volt=0.285855*intcode-0.5896118255011659
            return round(volt,3)

    # Convert User hex code to temp
    def hex2temp(hexval):
            intcode=hex10bitcode(hexval)
            volt=code2volt(intcode,5)
            voltdivider =(volt*65000)/(2.5-volt)
            temp=Tthermistor10k(voltdivider)
                return round(temp,2)

    # Convert User hex code to TEC voltage
    def hex2TECV(hexval):
            intcode=hex10bitcode(hexval)
            volt=code2volt(intcode,5)
                return round(volt,3)

    # Convert User hex code to TEC current
    def hex2TECI(hexval):
            intcode=hex10bitcode(hexval)
            volt=code2volt(intcode,5)
            current=volt/(0.05+0.27)
                return round(current,3)

    '''
    DAC testing
    '''
    # #Testing the HV functions
    # hv= int(raw_input('Set the High Voltage (V):\n'));

    # hvout = volt2hex( hv );
    # print "HV codeword: ", hvout


    # #Testing the temp functions
```

```
    # t= int(raw_input('Set the temperature (C):\n'));

    # tout = temp2hex( t );
    # print "Temperature codeword: ", tout

    # #Testing the temp functions
    # comp=int(raw_input('Set the comparitor threshold (mV):\n'));

    # compout = comp2hex( comp );
    # print "Comparitor threshold codeword: ", compout

    '''
    ADC testing
    '''
    # #Testing the HV readout
    # hv= raw_input('Readout the High Voltage:\n');
    # hvout = hex2volt( hv );
    # print "HV (V): ", hvout

    # #Testing the temperature readout
    # t= raw_input('Readout the temperature:\n');
    # tout = hex2temp( t );
    # print "Temp (C): ", tout

    # #Testing the TEC voltage readout
    # v= raw_input('Readout the TEC voltage:\n');
    # vout = hex2TECV( v );
    # print "TEC Voltage (V): ", vout

    # #Testing the TEC current readout
    # v= raw_input('Readout the TEC current:\n');
    # vout = hex2TECI( v );
    # print "TEC current (A): ", vout
```

Listing B.2: The Python program that runs the detectors. It uses the functions defined above and the inter-integrated circuit serial bus ($I^2C$) bus to communicate with the detectors.

```
import sys
import math
import array
import smbus
import i2chelp
import time
```

```
print "\n\ nInitializing the I2C controller ..."

bus = smbus.SMBus(1)

#Write a string of values to a register
def send_command(address,register,command):
    commandlength = len(command)
    #register = hex(register)
    listcommand = [int("".join([command[i],command[i+1]]),16) for i in xrange(0,commandlength
        -1,2)]

    #print[commandlength,address,type(address), register ,type( register ),command,type(command),
        listcommand,type(listcommand)]
    bus.write_i2c_block_data(address, register ,listcommand)

#read command
def read_command(address,register,length):
    return bus.read_i2c_block_data(address, register ,length)

# Ask user for the address (not gonna for now)

#address = int(raw_input("Enter the slave address of the controller as an hex number: "),16)
add_1=0x6a
add_2=0x6b
add_3=0x6c
add_4=0x6d
address=[add_1,add_2,add_3,add_4]

# Initialize the controller: send string 0A100900F0

initcode = [0x10,0x09,0x00,0xf0]
for i in xrange(0,4):
    bus.write_i2c_block_data(address[i],0x0A,initcode)
print "Done!\n"

channelnames = ['1','2','3','4','a','A']
singlechannel = ['1','2','3','4']

while True:
    print "-----------------------------------------------\
        nPlease choose one of the following menu options: \n
        -----------------------------------------------"
    print "V : Set a bias voltage"
    print "T : Set temperature"
    print "C : Set comparator threshold"
```

```
        print "1   :   Read TEC current"
        print "2   :   Read TEC voltage"
        print "3   :   Read high voltage"
        print "4   :   Read temperature"
        print "I   :    Initialize   the  detectors  to  standard  operating   settings"
        print "S   :   Shut down the detectors"
        print "Q   :   Quit the menu :("
        user_choice = raw_input("Choice: ")


    ###Setting the bias voltage
        if (user_choice == 'V') or (user_choice == 'v'):
            vchannel = raw_input("Please select a channel number (or a to set all at once): ")
            while vchannel not in channelnames:
                print "User error, bad channel number choice. Choose from [1,2,3,4, a]"
                vchannel = raw_input("Please select a channel number (or A to set all at once): ")
            if vchannel in singlechannel:
                vaddress=[address[int(vchannel)-1]]
            else:
                vaddress = address
                vchannel = singlechannel

            input_voltage = float(raw_input("Please enter a voltage (in V): "))

            for i in xrange(0,len(vaddress)):
                vcode = i2chelp.volt2hex(input_voltage,vchannel[i])
                send_command(vaddress[i],0x02,vcode)
                print 'Voltage on channel '+str(vchannel[i])+' set to '+str(input_voltage)+'V'
            print '\n'

    ###Setting the temperature
        elif (user_choice == 'T') or (user_choice == 't'):
            tchannel = raw_input("Please select a channel number (or a to set all at once): ")
            while tchannel not in channelnames:
                print "User error, bad channel number choice. Choose from [1,2,3,4, a]"
                tchannel = raw_input("Please select a channel number (or A to set all at once): ")
            if tchannel in singlechannel:
                taddress=[address[int(tchannel)-1]]
            else:
                taddress = address
                tchannel = singlechannel

            temperature = float(raw_input("Please enter a temperature (in deg C): "))

            tcode = i2chelp.temp2hex(temperature)
```

```
            print '\n'
            for i in xrange(0,len(taddress)):
                send_command(taddress[i],0x01,tcode)
                print 'Temperature on channel '+str(tchannel[i])+' set to '+str(temperature)+'C'
            print '\n'


        ######set comparitor threshold level
        elif (user_choice == 'C') or (user_choice == 'c'):
            cchannel = raw_input("Please select a channel number (or a to set all at once): ")
            while cchannel not in channelnames:
                print "User error, bad channel number choice. Choose from [1,2,3,4,a]"
                cchannel = raw_input("Please select a channel number (or A to set all at once): ")
            if cchannel in singlechannel:
                caddress=[address[int(cchannel)-1]]
            else:
                caddress = address
                cchannel = singlechannel

            comp_threshold = float(raw_input("Please enter a value for the comparator threshold (in
                mV): "))
            ccode = i2chelp.comp2hex(comp_threshold)
            print '\n'
            for i in xrange(0,len(caddress)):
                send_command(caddress[i],0x03,ccode)
                print 'Threshold on channel '+str(cchannel[i])+' set to '+str(comp_threshold)+'mV'
            print '\n'


        #####Read the TEC current
        elif user_choice == '1':
            ichannel = raw_input("Please select a channel number (or a to read all at once): ")
            while ichannel not in channelnames:
                print "User error, bad channel number choice. Choose from [1,2,3,4,a]"
                ichannel = raw_input("Please select a channel number (or A to set all at once): ")
            if ichannel in singlechannel:
                iaddress=[address[int(ichannel)-1]]
            else:
                iaddress = address
                ichannel = singlechannel
            print "Reading TEC current..."
            readicommand = '01'
            iread=range(len(iaddress))
            for i in xrange(0,len(iaddress)):
                send_command(iaddress[i],0x00,readicommand)
```

```
138             idata=read_command(iaddress[i],0x01,2)
                idata=i2chelp.hex2TECI(i2chelp. list2string (idata))
                iread[i] = ['Channel '+ str(ichannel[i])+': ',idata]

        print "\nResult: "
143     for i in xrange(0,len(iread)):
            print iread[i][0]+str(iread[i][1])+' A'
        print "\n"


148

    elif user_choice == '2':
        vchannel = raw_input("Please select a channel number (or a to read all at once): ")
        while vchannel not in channelnames:
153         print "User error, bad channel number choice. Choose from [1,2,3,4,a]"
            vchannel = raw_input("Please select a channel number (or A to set all at once): ")
        if vchannel in singlechannel:
            vaddress=[address[int(vchannel)-1]]
        else:
158         vaddress = address
            vchannel = singlechannel
        print "Reading TEC voltage..."
        readvcommand = '02'
        vread=range(len(vaddress))
163     for i in xrange(0,len(vaddress)):
            send_command(vaddress[i],0x00,readvcommand)
            vdata=read_command(vaddress[i],0x01,2)
            vdata=i2chelp.hex2TECV(i2chelp. list2string (vdata))
            vread[i] = ['Channel '+ str(vchannel[i])+': ',vdata]
168
        print "\nResult: "
        for i in xrange(0,len(vread)):
            print vread[i][0]+str(vread[i][1])+' V'
        print "\n"
173


    elif user_choice == '3':
        hvchannel = raw_input("Please select a channel number (or a to read all at once): ")
178     while hvchannel not in channelnames:
            print "User error, bad channel number choice. Choose from [1,2,3,4,a]"
            hvchannel = raw_input("Please select a channel number (or A to set all at once): ")
        if hvchannel in singlechannel:
            hvaddress=[address[int(hvchannel)-1]]
```

```
183             else:
                    hvaddress = address
                    hvchannel = singlechannel
                print "Reading high voltage ..."
                readHVcommand = '04'
188             HVread=range(len(hvaddress))
                for i in xrange(0,len(hvaddress)):
                    send_command(hvaddress[i],0x00,readHVcommand)
                    HVdata=read_command(hvaddress[i],0x01,2)
                    HVdata=i2chelp.hex2volt(i2chelp. list2string (HVdata),hvchannel[i])
193                 HVread[i] = ['Channel '+ str(hvchannel[i])+': ',HVdata]

                print "\nResult: "
                for i in xrange(0,len(HVread)):
                    print HVread[i][0]+str(HVread[i][1])+' V'
198             print "\n"

        #Reading out what the temperature is
            elif user_choice == '4':
                Tchannel = raw_input("Please select a channel number (or a to read all at once): ")
203             while Tchannel not in channelnames:
                    print "User error, bad channel number choice. Choose from [1,2,3,4,a]"
                    Tchannel = raw_input("Please select a channel number (or A to set all at once): ")
                if Tchannel in singlechannel:
                    Taddress=[address[int(Tchannel)-1]]
208             else:
                    Taddress = address
                    Tchannel = singlechannel
                print "Reading temperature..."
                readTcommand = '08'
213             Tread=range(len(Taddress))

                for i in xrange(0,len(Taddress)):
                    send_command(Taddress[i],0x00,readTcommand)
                    Tdata=read_command(Taddress[i],0x01,2)
218                 Tdata=i2chelp.hex2temp(i2chelp. list2string (Tdata))
                    Tread[i] = ['Channel '+ str(Tchannel[i])+': ',Tdata]

                print "\nResult: "
                for i in xrange(0,len(Tread)):
223                 print Tread[i][0]+str(Tread[i][1])+'C'
                print "\n"


        #Shutdown the channels
```

```
228         elif (user_choice == 'S') or (user_choice == 's'):
                print "Commencing shutdown procedures..."
                #set temps to 0:
                for i in xrange(0,len(address)):
                    send_command(address[i],0x01,'0000')
233                 print 'Temperature on channel '+str(singlechannel[i])+' set to room temp (25 C)'
                #set HV to 0:
                for i in xrange(0,len(address)):
                    send_command(address[i],0x02,'0000')
                    print 'Bias voltage on channel '+str(singlechannel[i])+' set to 0 V'
238             #set comparitor to 0:
                for i in xrange(0,len(address)):
                    send_command(address[i],0x03,'0000')
                    print 'Threshold on channel '+str(singlechannel[i])+' set to 0 mV'
                print "Done!"
243
        # Initialize the channels
            elif (user_choice == 'I') or (user_choice == 'i'):
                print "Commencing startup procedures..."
                #set temps to 0:
248             for i in xrange(0,len(address)):
                    send_command(address[i],0x01,'09C5')
                    time.sleep(8)
                    print 'Temperature on channel '+str(singlechannel[i])+' set to -20C'
                #set HV to 0:
253             workingvbias=[338,345,360,358]
                for i in xrange(0,len(address)):
                    send_command(address[i],0x02,i2chelp.volt2hex(workingvbias[i], singlechannel[i]))
                    print 'Bias voltage on channel '+str(singlechannel[i])+' set to '+str(workingvbias[i])
                #set comparitor to 150mV:
258             for i in xrange(0,len(address)):
                    send_command(address[i],0x03,'048B')
                    print 'Threshold on channel '+str(singlechannel[i])+' set to 50 mV'
                print "Done!"


263
            elif user_choice == 'Q' or 'q':
                print "Goodbye!"
                sys.exit()

268         else:
                print "Invalid option, try again."
```

# Acronyms

**I$^2$C** inter-integrated circuit serial bus. 60, 64–68, 80, 139

**ADC** analog to digital converter. 60, 63, 64, 66
**APD** avalanche photodiode. xiv, xvi, xix, 11–15, 60, 63–65, 108, 113–115, 117
**APT** Acquisition Pointing and Tracking. xvii, xviii, 58, 82, 83, 85, 87–99, 103, 127
**AR** anti-reflection. 85

**BB84** Bennett-Brassard 1984. x, 19, 20, 22, 23, 25, 35, 117
**BBM92** Bennett-Brassard-Mermin 1992. 22

**CAN** controller area network bus. 80
**CDPU** control and data processing unit. xi, 15, 59, 60, 66–68, 74, 80
**CSA** Canadian Space Agency. 31
**CW** continuous wave. 109, 116, 127

**DAC** digital-to-analog converter. 60, 63, 64, 66
**DC** direct current. 60
**DIQKD** device independent quantum key distribution. 19

**E91** Ekert 1991. 22
**EDFA** erbium-doped fiber amplifier. 119

**FLIR** FLIR Motion Control System. 90
**FOV** field-of-view. 8, 58, 86, 91, 92
**FWHM** full width half max. 10, 11, 96, 97

**GLAS** Geoscience Laser Altimeter System. 80
**GPS** Global Positioning System. 50, 51

**HV** high voltage. 63, 65

**IC** integrated circuit. 63, 64, 66
**ICESat** ice, cloud and land elevation satellite. 80
**InGaAs** Indium gallium arsenide. 11, 13, 14
**INO** Institut national d'optique. 88, 89, 103, 104
**IOA** Integrated Optical Assembly. xvi–xviii, 57, 58, 82–85, 87–94, 96, 98, 127
**IQC** Institute for Quantum Computing. 36, 98

**LIDAR** light detection and ranging. 8, 27
**LVDS** low voltage differential signal. 59, 63, 65, 66, 80

**MMF** multi-mode fiber. 59, 64, 72, 82, 85

**PCB** printed circuit board. xvi, 61, 63, 65, 66, 77, 78, 113
**PECL** Positive Emitter-Coupled Logic. 63
**PMT** photo multiplier tube. 10, 11
**PnPQKD** plug and play QKD. xviii, xix, 108, 116

**QBER** quantum bit error rate. xii, xviii, 29, 98–104
**QEYSSat** Quantum Encryption and Science Satellite. 80, 87, 98, 127
**QKD** Quantum Key Distribution. iii, iv, xv, xvi, xviii, 4, 7–9, 11, 17–20, 22–25, 27–33, 35, 38, 39, 44, 45, 51, 52, 54, 57, 58, 81, 86, 87, 98, 99, 102–109, 113, 116, 118, 125–128, 131, 147
**QKDR** quantum key distribution receiver. xi, xvi, 58, 65, 68, 70, 72, 77, 87, 127, 131
**QRNG** quantum random number generator. 19

**SLiK** super low K avalanche photodiode. xvi, 59, 64, 65, 75, 78, 80
**SM** single mode. xviii, xix, 107, 110
**SPAD** single photon avalanche photodiode. iii, 13, 14, 59, 60, 63–65, 69, 75, 106, 148
**SPDC** spontaneous parametric down conversion. 29, 30
**SSL** secure sockets layer. 3
**Stratos** Canadian Space Agency's stratospheric balloon program. xi, xiv, xv, 31–34, 41, 44, 45

**TEC** thermoelectric controller. 60, 63–67, 79
**TTL** transistor-transistor logic. 14

**USD** unambiguous state discrimination. 25, 26, 123

**WCP** weak coherent pulse. 116
**WiFi** wireless local area network. xvi, 50, 51, 54

# Glossary

**annihilation operator** ($\hat{a}$) The annihilation operator ($\hat{a}$) is defined as $\frac{1}{\sqrt{2}}(q + \mathbf{i}p)$ where $q, p$ are the cannonical position and momentum operators in quantum mechanics [178].. 5, 6

**breakdown voltage** The breakdown voltage of an single photon avalanche photodiode (SPAD) is a physical property of the diode, which is described as the minimum required reverse bias on the diode that allows avalanches to be triggered [50].. xi, xiv, 12, 13, 69, 70

**ciphertext** Ciphertext is the output of an encryption protocol that scrambles a plain text with a key in some algorithmic fashion [17].. 3, 148

**creation operator** ($\hat{a}^\dagger$) The creation operator ($\hat{a}^\dagger$) is defined as $\frac{1}{\sqrt{2}}(q - \mathbf{i}p)$ where $q, p$ are the cannonical position and momentum operators in quantum mechanics [178].. 5, 6

**cryptographic hash** A way of taking an arbirtrary message and scrambling it and reducing it to a fixed size, and there should not be two different messages with the same reduced message (called the hash). Importantly it should be a one-way function that is impossible to recondtruct the longer message from the hash [179], plural=cryptographic hashes. 3

**Fock state** ($|n\rangle$) An eigen state of the number operator $\hat{n}$ [178].. 5, 6

**key** A cryptographic key is a parmeter (usually a random bit string) that determines the output of a cryptographic protocol [179]. Keys are required for transforming plain text to ciphertext in encryption protocols.. 2, 3, 148

**mean photon number** ($\mu$) The mean photon number of a state $|\psi\rangle$ is calculated by $\langle\psi|\,\hat{a}^\dagger\hat{a}\,|\psi\rangle$. For Fock or number states, the mean photon number is just the number of photons in the state as a mean refers to a distribution [178].. 106, 108

**number operator** ($\hat{n}$) An operator for quantum oscillator physics, and describes the number of photons in a chosen mode of a system. $\hat{n} \equiv \hat{a}^\dagger \hat{a}$ [178].. 5

**plain text** The content of a message stored or sent in an encryption protocol [17].. 2, 3, 148

# References


[1] George Lucas. Star Wars: Episode IV - A New Hope, May 1977. IMDB ID: tt0076759 IMDB Rating: 8.7 (908,085 votes).

[2] Richard Marquand. Star Wars: Episode VI - Return of the Jedi, May 1983. IMDB ID: tt0086190 IMDB Rating: 8.4 (679,733 votes).

[3] J. J. Abrams. Star Wars: The Force Awakens, December 2015. IMDB ID: tt2488496 IMDB Rating: 8.2 (561,678 votes).

[4] Understanding Web Site Certificates — US-CERT. https://www.us-cert.gov/ncas/tips/ST05-010.

[5] Improving SSL warnings [APF talk Jan 2015]. https://docs.google.com/presentation/d/1TNFx6eaQVfe83PV80-FZ39QY1dSLGCWW8f2i5-NeJ48/present?usp=embed_facebook.

[6] NIST.gov - Computer Security Division - Computer Security Resource Center. http://csrc.nist.gov/groups/ST/toolkit/random_number.html.

[7] Information Technology Laboratory. Digital Signature Standard (DSS). Technical Report NIST FIPS 186-4, National Institute of Standards and Technology, July 2013.

[8] OneRNG. http://www.moonbaseotago.com/onerng/.

[9] waywardgeek/infnoise. https://github.com/waywardgeek/infnoise.

[10] Donald E. Knuth. *Art of Computer Programming, Volume 2: Seminumerical Algorithms*. Addison-Wesley Professional, May 2014.

[11] Ralph C. Merkle. Secure Communications over Insecure Channels. *Commun. ACM*, 21(4):294–299, April 1978.

[12] Public Key Infrastructure (Windows). https://msdn.microsoft.com/en-us/library/windows/desktop/bb427432%28v=vs.85%29.aspx?f=255&MSPPError=-2147217396.

[13] C. E. Shannon. Communication theory of secrecy systems. *The Bell System Technical Journal*, 28(4):656–715, October 1949.

[14] Gilbert S. Vernam. Secret signaling system, July 1919. U.S. Classification 380/33, 380/26, 380/259; Cooperative Classification H04K1/00, H04L9/00.

[15] Black Hat USA 2014. https://www.blackhat.com/us-14/briefings.html#badusb-on-accessories-that-turn-evil.

[16] Heartbleed Bug. http://heartbleed.com/.

[17] Jonathan Katz and Yehuda Lindell. *Introduction to Modern Cryptography: Principles and Protocols*. CRC Press, August 2007.

[18] Adi Shamir. How to Share a Secret. *Commun. ACM*, 22(11):612–613, November 1979.

[19] David Chaum, Claude Crépeau, and Ivan Damgard. Multiparty Unconditionally Secure Protocols. In *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing*, STOC '88, pages 11–19, New York, NY, USA, 1988. ACM.

[20] C. H. Bennett and G. Brassard. Quantum Cryptography: Public Key Distribution and Coin Tossing. In *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing*, pages 175–179, Bangalore, India, December 1984.

[21] T. Lunghi, J. Kaniewski, F. Bussières, R. Houlmann, M. Tomamichel, A. Kent, N. Gisin, S. Wehner, and H. Zbinden. Experimental Bit Commitment Based on Quantum Communication and Special Relativity. *Phys. Rev. Lett.*, 111(18):180504, November 2013.

[22] D. A. Redman, S. Brown, R. H. Sands, and S. C. Rand. Spin dynamics and electronic states of N- \textit{V} centers in diamond by EPR and four-wave-mixing spectroscopy. *Phys. Rev. Lett.*, 67(24):3420–3423, December 1991.

[23] G. D. Fuchs, V. V. Dobrovitski, R. Hanson, A. Batra, C. D. Weis, T. Schenkel, and D. D. Awschalom. Excited-State Spectroscopy Using Single Spin Manipulation in Diamond. *Phys. Rev. Lett.*, 101(11):117601, September 2008.

[24] Alexandre Zagoskin and Alexandre Blais. Superconducting qubits. *arXiv:0805.0164 [cond-mat]*, May 2008.

[25] M. H. Devoret, A. Wallraff, and J. M. Martinis. Superconducting Qubits: A Short Review. *arXiv:cond-mat/0411174*, November 2004.

[26] Yuriy Makhlin, Gerd Schön, and Alexander Shnirman. Quantum-state engineering with Josephson-junction devices. *Rev. Mod. Phys.*, 73(2):357–400, May 2001.

[27] N. N. Ledentsov, V. M. Ustinov, V. A. Shchukin, P. S. Kop'ev, Zh I. Alferov, and D. Bimberg. Quantum dot heterostructures: Fabrication, properties, lasers (Review). *Semiconductors*, 32(4):343–365, April 1998.

[28] M. A. Reed, J. N. Randall, R. J. Aggarwal, R. J. Matyi, T. M. Moore, and A. E. Wetsel. Observation of discrete electronic states in a zero-dimensional semiconductor nanostructure. *Phys. Rev. Lett.*, 60(6):535–537, February 1988.

[29] A. Imamog¯lu, D. D. Awschalom, G. Burkard, D. P. DiVincenzo, D. Loss, M. Sherwin, and A. Small. Quantum Information Processing Using Quantum Dot Spins and Cavity QED. *Phys. Rev. Lett.*, 83(20):4204–4207, November 1999.

[30] Pieter Kok, W. J. Munro, Kae Nemoto, T. C. Ralph, Jonathan P. Dowling, and G. J. Milburn. Linear optical quantum computing with photonic qubits. *Rev. Mod. Phys.*, 79(1):135–174, January 2007.

[31] E. Knill, R. Laflamme, and G. J. Milburn. A scheme for efficient quantum computation with linear optics. *Nature*, 409(6816):46–52, January 2001.

[32] Kyo Inoue, Edo Waks, and Yoshihisa Yamamoto. Differential Phase Shift Quantum Key Distribution. *Phys. Rev. Lett.*, 89(3):037902, June 2002.

[33] 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(1):41, 2002.

[34] I. Marcikic, H. de Riedmatten, W. Tittel, H. Zbinden, M. Legré, and N. Gisin. Distribution of Time-Bin Entangled Qubits over 50 km of Optical Fiber. *Phys. Rev. Lett.*, 93(18):180502, October 2004.

[35] T. Honjo, H. Takesue, H. Kamada, Y. Nishida, O. Tadanaga, M. Asobe, and K. Inoue. Long-distance distribution of time-bin entangled photon pairs over 100 km using frequency up-conversion detectors. *Optics Express*, 15(21):13957, 2007.

[36] Matthieu Bloch, Steven W. McLaughlin, Jean-Marc Merolla, and Frédéric Patois. Frequency-coded quantum key distribution. *Optics Letters*, 32(3):301, February 2007.

[37] Mohammad Mirhosseini, Omar S. Magaña-Loaiza, Malcolm N. O'Sullivan, Brandon Rodenburg, Mehul Malik, Martin P. J. Lavery, Miles J. Padgett, Daniel J. Gauthier, and Robert W. Boyd. High-dimensional quantum cryptography with twisted light. *New J. Phys.*, 17(3):033033, 2015.

[38] Nurul T. Islam, Clinton Cahall, Andres Aragoneses, Charles C. Lim, Michael S. Allman, Varun Verma, Sae Woo Nam, Jungsang Kim, and Daniel J. Gauthier. Discrete-variable time-frequency quantum key distribution. page FTh3C.3. OSA, 2016.

[39] Paul Kwiat, Bradley Christensen, Kevin McCusker, Daniel Kumor, and Daniel Gauthier. High Data Rate Quantum Cryptography. May 2015.

[40] Richard P. Feynman. *Statistical Mechanics: A Set Of Lectures*. Westview Press, March 1998.

[41] David Jeffery Griffiths. Introduction to Quantum Mechanics. https://books.google.ca/books?id=9sqIaRGx_EoC&dq=griffiths+quantum+mechanics&hl=en&sa=X&ved=0ahUKEwj7ns3DktjNAhUF6YMKHaAbAjkQ6AEIGzAA.

[42] Jean-Philippe Bourgoin. *Experimental and theoretical demonstration of the feasibility of global quantum cryptography using satellites*. PhD thesis, October 2014.

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

[44] Bahaa E. A. Saleh, Malvin Carl Teich. Fundamentals of Photonics, 2nd Edition. http://ca.wiley.com/WileyCDA/WileyTitle/productCd-0471358320.html.

[45] Eugene Hecht. *Optics*. Pearson Education, July 2015.

[46] J. Brendel, N. Gisin, W. Tittel, and H. Zbinden. Pulsed Energy-Time Entangled Twin-Photon Source for Quantum Communication. *Phys. Rev. Lett.*, 82(12):2594–2597, March 1999.

[47] Paul D Townsend, JG Rarity, and PR Tapster. Single photon interference in 10 km long optical fibre interferometer. *Electronics Letters*, 29(7):634–635, 1993.

[48] D. Stucki, C. Barreiro, S. Fasel, J.-D. Gautier, O. Gay, N. Gisin, R. Thew, Y. Thoma, P. Trinkler, F. Vannel, and H. Zbinden. Continuous high speed coherent one-way quantum key distribution. *Opt. Express*, 17(16):13326–13334, 2009.

[49] J.-P. Bourgoin, E. Meyer-Scott, B. L. Higgins, B. Helou, C. Erven, H. Huebel, B. Kumar, D. Hudson, I. D'Souza, R. Girard, R. Laflamme, and T. Jennewein. A comprehensive design and performance analysis of LEO satellite quantum communication. *New Journal of Physics*, 15(2):023006, February 2013.

[50] A. Migdall, S.V. Polyakov, J. Fan, and J.C. Bienfang. *Single-Photon Generation and Detection: Physics and Applications*. Experimental Methods in the Physical Sciences. Elsevier Science, 2013.

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

[52] Martin A. Green and Mark J. Keevers. Optical properties of intrinsic silicon at 300 K. *Prog. Photovolt: Res. Appl.*, 3(3):189–192, January 1995.

[53] G. C. Osbourn. ${\mathrm{In}}_{x}{\mathrm{Ga}}_{1-x}\mathrm{As}-{\mathrm{In}}_{y}{\mathrm{Ga}}_{1-y}\mathrm{As}$ strained-layer superlattices: A proposal for useful, new electronic materials. *Phys. Rev. B*, 27(8):5126–5128, April 1983.

[54] T. Pearsall, M. Piskorski, A. Brochet, and J. Chevrier. A Ga0.47In0.53As/InP heterophotodiode with reduced dark current. *IEEE Journal of Quantum Electronics*, 17(2):255–259, February 1981.

[55] T. P. Pearsall, R. A. Logan, and C. G. Bethea. GaInAs/InP large bandwidth (> 2 GHz) PIN detectors. *Electronics Letters*, 19(16):611–612, August 1983.

[56] 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.

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

[58] Dagmar Bruß and Norbert Lütkenhaus. Quantum key distribution: from principles to practicalities. *Applicable Algebra in Engineering, Communication and Computing*, 10(4-5):383–399, 2000.

[59] Renato Renner, Nicolas Gisin, and Barbara Kraus. Information-theoretic security proof for quantum-key-distribution protocols. *Phys. Rev. A*, 72(1):012332, July 2005.

[60] Christopher A. Fuchs and Jeroen van de Graaf. Cryptographic Distinguishability Measures for Quantum Mechanical States. *arXiv:quant-ph/9712042*, December 1997.

[61] Jörn Müller-Quade and Renato Renner. Composability in quantum cryptography. *New J. Phys.*, 11(8):085006, 2009.

[62] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, December 2010.

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

[64] Hoi-Kwong Lo, Marcos Curty, and Bing Qi. Measurement-Device-Independent Quantum Key Distribution. *Phys. Rev. Lett.*, 108(13):130503, March 2012.

[65] Marcos Curty. Device-Independent Quantum Key Distribution. page JTh4K.6. OSA, 2012.

[66] Antonio Acin. Device-Independent Quantum Key Distribution. page FF1A.1. OSA, 2015.

[67] Esther Hänggi. Device-independent quantum key distribution. *arXiv:1012.3878 [quant-ph]*, December 2010.

[68] Miguel Herrero-Collantes and Juan Carlos Garcia-Escartin. Quantum Random Number Generators. *arXiv:1604.03304 [quant-ph]*, April 2016.

[69] Renato Renner and Robert König. Universally Composable Privacy Amplification Against Quantum Adversaries. In Joe Kilian, editor, *Theory of Cryptography*, number 3378 in Lecture Notes in Computer Science, pages 407–425. Springer Berlin Heidelberg, February 2005.

[70] Artur K. Ekert. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.*, 67(6):661–663, August 1991.

[71] Charles H. Bennett, Gilles Brassard, and N. David Mermin. Quantum cryptography without Bell's theorem. *Phys. Rev. Lett.*, 68(5):557–559, February 1992.

[72] Eli Biham, Michel Boyer, Gilles Brassard, Jeroen van de Graaf, and Tal Mor. Security of Quantum Key Distribution Against All Collective Attacks. *arXiv:quant-ph/9801022*, January 1998.

[73] Dominic Mayers. Unconditional Security in Quantum Cryptography. *J. ACM*, 48(3):351–406, May 2001.

[74] Hoi-Kwong Lo and H. F. Chau. Unconditional Security of Quantum Key Distribution over Arbitrarily Long Distances. *Science*, 283(5410):2050–2056, March 1999.

[75] Reviews of Modern Physics - Accepted Paper: Quantum memories at finite temperature. https://journals.aps.org/rmp/accepted/94070E73M2c12e0ff01049830b49376bb4dcdeaab.

[76] Philippe Grangier, Juan Ariel Levenson, and Jean-Philippe Poizat. Quantum non-demolition measurements in optics. *Nature*, 396(6711):537–542, December 1998.

[77] John Kelsey, Bruce Schneier, David Wagner, and Chris Hall. Cryptanalytic Attacks on Pseudorandom Number Generators. In Serge Vaudenay, editor, *Fast Software Encryption*, number 1372 in Lecture Notes in Computer Science, pages 168–188. Springer Berlin Heidelberg, March 1998.

[78] SST: TEMPEST Standards SDIP 27 Level A, Level B & AMSG 784, 720B, 788A. http://www.sst.ws/tempest_standards.php.

[79] 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, February 2006.

[80] Fu-Guo Deng, Xi-Han Li, Hong-Yu Zhou, and Zhan-jun Zhang. Improving the security of multiparty quantum secret sharing against Trojan horse attack. *Phys. Rev. A*, 72(4):044302, October 2005.

[81] Fu-Guo Deng, Ping Zhou, Xi-Han Li, Chun-Yan Li, and Hong-Yu Zhou. Robustness of two-way quantum communication protocols against Trojan horse attack. *arXiv:quant-ph/0508168*, August 2005.

[82] Understanding Denial-of-Service Attacks — US-CERT. https://www.us-cert.gov/ncas/tips/ST04-015.

[83] Bing Qi, Chi-Hang Fred Fung, Hoi-Kwong Lo, and Xiongfeng Ma. Time-shift attack in practical quantum cryptosystems. *arXiv:quant-ph/0512080*, December 2005.

[84] Chi-Hang Fred Fung, Bing Qi, Kiyoshi Tamaki, and Hoi-Kwong Lo. Phase-remapping attack in practical quantum-key-distribution systems. *Phys. Rev. A*, 75(3):032314, March 2007.

[85] Gilles Brassard, Norbert Lütkenhaus, Tal Mor, and Barry C. Sanders. Limitations on Practical Quantum Cryptography. *Phys. Rev. Lett.*, 85(6):1330–1333, August 2000.

[86] Lars Lydersen, Carlos Wiechers, Christoffer Wittmann, Dominique Elser, Johannes Skaar, and Vadim Makarov. Thermal blinding of gated detectors in quantum cryptography. *Optics Express*, 18(26):27938, December 2010.

[87] Marcos Curty and Norbert Lütkenhaus. Intercept-resend attacks in the Bennett-Brassard 1984 quantum-key-distribution protocol with weak coherent pulses. *Phys. Rev. A*, 71(6):062301, June 2005.

[88] F. Callegati, W. Cerroni, and M. Ramilli. Man-in-the-Middle Attack to the HTTPS Protocol. *IEEE Security Privacy*, 7(1):78–81, January 2009.

[89] Miloslav Dušek, Mika Jahma, and Norbert Lütkenhaus. Unambiguous state discrimination in quantum cryptography with weak coherent states. *Phys. Rev. A*, 62(2):022306, July 2000.

[90] Charles H. Bennett, François Bessette, Gilles Brassard, Louis Salvail, and John Smolin. Experimental quantum cryptography. *J. Cryptology*, 5(1):3–28, January 1992.

[91] Anthony Chefles and Stephen M. Barnett. Optimum unambiguous discrimination between linearly independent symmetric states. *Physics Letters A*, 250(4):223–229, December 1998.

[92] Haris Riris, Kenji Numata, Steve Li, Stewart Wu, Anand Ramanathan, Martha Dawsey, Jianping Mao, Randolph Kawa, and James B. Abshire. Airborne measurements of atmospheric methane column abundance using a pulsed integrated-path differential absorption lidar. *Applied Optics*, 51(34):8296, December 2012.

[93] James B. Abshire, Anand Ramanathan, Haris Riris, Jianping Mao, Graham R. Allan, William E. Hasselbrack, Clark J. Weaver, and Edward V. Browell. Airborne Measurements of CO2 Column Concentration and Range Using a Pulsed Direct-Detection IPDA Lidar. *Remote Sensing*, 6(1):443–469, December 2013.

[94] National Oceanic US Department of Commerce and Atmospheric Administration. What is LIDAR. http://oceanservice.noaa.gov/facts/lidar.html.

[95] Hyperion Project. http://projecthyperion.co.uk/.

[96] Kenichi Araki, Yoshinori Arimoto, Motokazu Shikatani, Masahiro Toyoda, Morio Toyoshima, Tetsuo Takahashi, Seiji Kanda, and Koichi Shiratama. Performance evaluation of laser communication equipment onboard the ETS-VI satellite. volume 2699, pages 52–59, 1996.

[97] Toni Tolker-Nielsen and Gotthard Oppenhauser. In-orbit test result of an operational optical intersatellite link between ARTEMIS and SPOT4, SILEX. volume 4635, pages 1–15, 2002.

[98] Renny Fields, Carl Lunde, Robert Wong, Josef Wicker, David Kozlowski, John Jordan, Brian Hansen, Gerd Muehlnikel, Wayne Scheel, Uwe Sterr, Ralph Kahle, and Rolf Meyer. NFIRE-to-TerraSAR-X laser communication results: satellite pointing, disturbances, and other attributes consistent with successful performance. volume 7330, pages 73300Q–73300Q–15, 2009.

[99] European Commission : CORDIS : Projects & Results Service : advanced Concept for laser uplink/ downlink CommuniCation with sPace Objects. http://cordis.europa.eu/project/rcn/193508_en.html.

[100] A. Gomez, K. Shi, C. Quintana, M. Sato, G. Faulkner, B. C. Thomsen, and D. O'Brien. Beyond 100-Gb/s Indoor Wide Field-of-View Optical Wireless Communications. *IEEE Photonics Technology Letters*, 27(4):367–370, February 2015.

[101] Patrick Hamill, Laura T. Iraci, Emma L. Yates, Warren Gore, T. Paul Bui, Tomoaki Tanaka, and Max Loewenstein. A New Instrumented Airborne Platform for Atmospheric Research. *Bull. Amer. Meteor. Soc.*, 97(3):397–404, July 2015.

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

[103] W. T. Buttler, R. J. Hughes, P. G. Kwiat, S. K. Lamoreaux, G. G. Luther, G. L. Morgan, J. E. Nordholt, C. G. Peterson, and C. M. Simmons. Practical free-space quantum key distribution over 1 km. *Physical Review Letters*, 81(15):3283–3286, October 1998.

[104] Richard J Hughes, William T Buttler, Paul G Kwiat, Steve K Lamoreaux, George L Morgan, Jane E Nordholt, and C Glen Peterson. Practical quantum cryptography for secure free-space communications. *arXiv preprint quant-ph/9905009*, 1999.

[105] 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(24):5652–5655, June 2000.

[106] J.G. Rarity, P.M. Gorman, and P.R. Tapster. Secure key exchange over 1.9 km free-space range using quantum cryptography. *Electronics Letters*, 37(8):512–514.

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

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

[109] Cheng-Zhi Peng, Tao Yang, Xiao-Hui Bao, Jun Zhang, Xian-Min Jin, Fa-Yong Feng, Bin Yang, Jian Yang, Juan Yin, Qiang Zhang, Nan Li, Bao-Li Tian, and Jian-Wei Pan. Experimental Free-Space Distribution of Entangled Photon Pairs Over 13 km: Towards Satellite-Based Global Quantum Communication. *Phys. Rev. Lett.*, 94(15):150501, April 2005.

[110] Ivan Marcikic, Antía Lamas-Linares, and Christian Kurtsiefer. Free-space quantum key distribution with entangled photons. *Applied Physics Letters*, 89(10):101122, September 2006.

[111] 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, July 2007.

[112] Sebastian Nauerth, Florian Moll, Markus Rau, Christian Fuchs, Joachim Horwath, Stefan Frick, and Harald Weinfurter. Air-to-ground quantum communication. *Nature Photonics*, 7(5):382–386, 2013.

[113] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Du\u sek, N. Lütkenhaus, and M. Peev. The security of practical quantum key distribution. *RMP*, 81:1301–1350, 2009.

[114] Jian-Yu Wang, Bin Yang, Sheng-Kai Liao, Liang Zhang, Qi Shen, Xiao-Fang Hu, Jin-Cai Wu, Shi-Ji Yang, Hao Jiang, Yan-Lin Tang, Bo Zhong, Hao Liang, Wei-Yue Liu,

Yi-Hua Hu, Yong-Mei Huang, Bo Qi, Ji-Gang Ren, Ge-Sheng Pan, Juan Yin, Jian-Jun Jia, Yu-Ao Chen, Kai Chen, Cheng-Zhi Peng, and Jian-Wei Pan. Direct and full-scale experimental verifications towards ground-satellite quantum key distribution. *Nat Photon*, 7(5):387–393, May 2013.

[115] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner. Tight Finite-Key Analysis for Quantum Cryptography. *Nat. Commun.*, 3:634, 2012.

[116] Charles Ci Wen Lim, Marcos Curty, Nino Walenta, Feihu Xu, and Hugo Zbinden. Concise security bounds for practical decoy-state quantum key distribution. *Phys. Rev. A*, 89(2):022307, February 2014.

[117] Tang Zhongkan, Rakhitha Chandrasekara, Yau Yong Sean, Cliff Cheng, Christoph Wildfeuer, and Alexander Ling. Near-space flight of a correlated photon system. *arXiv:1404.3971 [physics, physics:quant-ph]*, April 2014.

[118] James A. Grieve, Robert Bedington, and Alexander Ling. Extreme environmental testing of a rugged correlated photon source. *arXiv:1504.00171 [physics, physics:quant-ph]*, April 2015.

[119] Feng Zengkun. Singapore-made device survives rocket explosion. http://www.straitstimes.com/singapore/singapore-made-device-survives-rocket-explosion, 2015-08-27T05:00:00+08:00.

[120] Zhongkan Tang, Rakhitha Chandrasekara, Yue Chuan Tan, Cliff Cheng, Luo Sha, Goh Cher Hiang, Daniel Oi, and Alexander Ling. Generation and analysis of correlated pairs of photons on board a nanosatellite. *arXiv:1603.06659 [physics, physics:quant-ph]*, March 2016.

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

[122] Eric C. Bellm, Jeng-Lun Chiu, Steven E. Boggs, Hsiang-Kuang Chang, Yuan-Hann Chang, Minghuey A. Huang, Mark Amman, Mark S. Bandstra, Wei-Che Hung, Pierre Jean, Jau-Shian Liang, Chih-Hsun Lin, Zhong-Kai Liu, Paul N. Luke, Daniel Perez-Becker, Ray-Shine Run, and Andreas Zoglauer. The 2010 balloon campaign of the Nuclear Compton Telescope. volume 7732, pages 773224–773224–9, 2010.

[123] Meir Pachter and Michael W. Oppenheimer. Adaptive optics for airborne platforms—Part 1: modeling. *Optics & Laser Technology*, 34(2):143–158, March 2002.

[124] 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(5):052339, November 2015.

[125] J.-P. Bourgoin, N. Gigov, B. L. Higgins, Z. Yan, E. Meyer-Scott, A. Khandani, N. L\" utkenhaus, and T. Jennewein. Experimentally simulating quantum key distribution with ground-to-satellite channel losses and processing limitations. 2015. In preparation.

[126] EV FERN Ltd.

[127] Donal P. Finegan, Mario Scheel, James B. Robinson, Bernhard Tjaden, Ian Hunt, Thomas J. Mason, Jason Millichamp, Marco Di Michiel, Gregory J. Offer, Gareth Hinds, Dan J.L. Brett, and Paul R. Shearing. In-operando high-speed tomography of lithium-ion batteries during thermal runaway. *Nat Commun*, 6, April 2015.

[128] Government of Canada Transport Canada Safety and Security Group. Aircraft Maintenance and Manufacturing. https://www.tc.gc.ca/eng/civilaviation/standards/maintenance-menu.htm, May 2010.

[129] Austin Roorda. Adaptive optics for studying visual function: a comprehensive review. *J Vis*, 11(7), 2011.

[130] Richard Davies and Markus Kasper. Adaptive Optics for Astronomy. *Annual Review of Astronomy and Astrophysics*, 50(1):305–351, 2012.

[131] R.K. Tyson. *Principles of Adaptive Optics, Fourth Edition*. CRC Press, 2015.

[132] QKDR Final Report. Technical Report QKDR-TN-005-IQC_9F063-120711, February 2015.

[133] APT Detailed Design Final Report. Technical Report IN0-133040-0004 N/A, June 2015.

[134] Photon Counting Detectors — PicoQuant. https://www.picoquant.com/products/category/photon-counting-detectors.

[135] Photon counting:Application technology — Hamamatsu Photonics. https://www.hamamatsu.com/us/en/technology/innovation/photoncounting/index.html.

[136] Single Photon Counting Modules SPCM. http://www.excelitas.com/pages/product/Single-Photon-Counting-Modules-SPCM.aspx.

[137] Photon Counting Modules from ID Quantique, 2015-01-29T16:06:03+00:00.

[138] Elena Anisimova, Dr. Jean-Philippe Bourgoin, Nikolay Gigov, Dr. Brendon Higgins, Catherine Holloway, Dr. Thomas Jennewein, Sarah Kaiser, Vadim Makarov, and Nigar Sultana. QKDR Requirements Document. Technical Report QKDR-TN-001-IQC_9F063-120711, November 2014.

[139] W. H. P. Pernice, C. Schuck, O. Minaeva, M. Li, G. N. Goltsman, A. V. Sergienko, and H. X. Tang. High-speed and high-efficiency travelling wave single-photon detectors embedded in nanophotonic circuits. *Nat Commun*, 3:1325, December 2012.

[140] Thierry Georges. Study of the non-Gaussian timing jitter statistics induced by soliton interaction and filtering. *Optics Communications*, 123(4):617–623, February 1996.

[141] Elena Anisimova, Jean-Philippe Bourgoin, Nikolay Gigov, Brendon Higgins, Catherine Holloway, Thomas Jennewein, Sarah Kaiser, Vadim Makarov, and Nigar Sultana. QKDR Detector Radiation Qualification Document. Technical Report QKDR-TN-004-IQC_9F063-120711, November 2014.

[142] H. Dautet, P. Deschamps, B. Dion, A. D. MacGregor, D. MacSween, R. J. McIntyre, C. Trottier, and P. P. Webb. Photon counting techniques with silicon avalanche photodiodes. *Appl. Opt.*, 32(21):3894–3900, 1993.

[143] Benjamin A. Prichard Jr. Mechanisms of electrical discharges in high vacuum at voltages up to 400 000 V. *Journal of Applied Physics*, 44(10):4548–4554, October 1973.

[144] Elena Anisimova, Jean-Philippe Bourgoin, Nikolay Gigov, Brendon Higgins, Catherine Holloway, Thomas Jennewein, Sarah Kaiser, Vadim Makarov, and Nigar Sultana. QKDR Detailed Design Document. Technical Report QKDR-TN-003-IQC_9F063-120711, April 2014.

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

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

[147] Nicolas Brunner, Daniel Cavalcanti, Stefano Pironio, Valerio Scarani, and Stephanie Wehner. Bell nonlocality. *Rev. Mod. Phys.*, 86(2):419–478, April 2014.

[148] Norbert Lütkenhaus. Estimates for practical quantum cryptography. *Phys. Rev. A*, 59(5):3301–3319, May 1999.

[149] J. SCIALDONE. An estimate of the outgassing of space payloads and its gaseous influence on the environment. *Journal of Spacecraft and Rockets*, 23(4):373–378, 1986.

[150] Thom Shanker. Navy Deploying Laser Weapon Prototype in Persian Gulf. *The New York Times*, April 2013.

[151] QEYSSAT APT Study Conceptual Design Document. Technical Report DDD-QES-M-0002, Rev P2.

[152] APT Requirements Technical Note. Technical Report IQC-APT-REQ-1001_9F063-120711, May 2015.

[153] APT Test and Demonstration Plan. Technical Report APT-TN-001-IQC_9F063-120711, June 2015.

[154] David JC MacKay and Radford M Neal. Near Shannon limit performance of low density parity check codes. *Electronics letters*, 32(18):1645–1646, 1996.

[155] Thomas Holenstein, Ueli Maurer, and Johan Sjödin. Complete Classification of Bilinear Hard-Core Functions. In Matthew Franklin, editor, *Advances in Cryptology — CRYPTO 2004*, volume 3152 of *Lecture Notes in Computer Science*, pages 73–91. Springer-Verlag, August 2004.

[156] M. Lucamarini, K. A. Patel, J. F. Dynes, B. Fröhlich, A. W. Sharpe, A. R. Dixon, Z. L. Yuan, R. V. Penty, and A. J. Shields. Efficient decoy-state quantum key distribution with quantified security. *Optics Express*, 21(21):24550, October 2013.

[157] Test Report APT Unit #2. Technical Report INO-133040-0012 NIA, September 2015.

[158] 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(7):070503, February 2014.

[159] Michael G. Tanner, Vadim Makarov, and Robert H. Hadfield. Optimised quantum hacking of superconducting nanowire single-photon detectors. *Optics Express*, 22(6):6734, March 2014.

[160] Clavis QKD for research and development applications, 2015-01-29T16:06:03+00:00.

[161] N. Walenta, A. Burg, D. Caselunghe, J. Constantin, N. Gisin, O. Guinnard, R. Houlmann, P. Junod, B. Korzh, N. Kulesza, M Legré, C. W. Lim, T. Lunghi, L. Monat, C. Portmann, M. Soucarros, R. T. Thew, P. Trinkler, G. Trolliet, F. Vannel, and H Zbinden. A fast and versatile quantum key distribution system with hardware key distillation and wavelength multiplexing. *New J. Phys.*, 16(1):013047, 2014.

[162] Yan-Lin Tang, Hua-Lei Yin, Si-Jing Chen, Yang Liu, Wei-Jun Zhang, Xiao Jiang, Lu Zhang, Jian Wang, Li-Xing You, Jian-Yu Guan, Dong-Xu Yang, Zhen Wang, Hao Liang, Zhen Zhang, Nan Zhou, Xiongfeng Ma, Teng-Yun Chen, Qiang Zhang, and Jian-Wei Pan. Measurement-Device-Independent Quantum Key Distribution over 200 km. *Phys. Rev. Lett.*, 113(19):190501, November 2014.

[163] Paul Jouguet, Sébastien Kunz-Jacques, Anthony Leverrier, Philippe Grangier, and Eleni Diamanti. Experimental demonstration of long-distance continuous-variable quantum key distribution. *Nat Photon*, 7(5):378–381, May 2013.

[164] Robert J. Collins, Ross J. Donaldson, Vedran Dunjko, Petros Wallden, Patrick J. Clarke, Erika Andersson, John Jeffers, and Gerald S. Buller. Realization of Quantum Digital Signatures without the Requirement of Quantum Memory. *Phys. Rev. Lett.*, 113(4):040502, July 2014.

[165] W. P. Grice, P. G. Evans, B. Lawrie, M. Legré, P. Lougovski, W. Ray, B. P. Williams, B. Qi, and A. M. Smith. Two-Party secret key distribution via a modified quantum secret sharing protocol. *Optics Express*, 23(6):7300, March 2015.

[166] B. Huttner, N. Imoto, N. Gisin, and T. Mor. Quantum cryptography with coherent states. *Phys. Rev. A*, 51(3):1863–1869, March 1995.

[167] Horace P. Yuen. Quantum amplifiers, quantum duplicators and quantum cryptography. *Quantum Semiclass. Opt.*, 8(4):939, 1996.

[168] Vadim Makarov, Jean-Philippe Bourgoin, Poompong Chaiwongkhot, Mathieu Gagne, Thomas Jennewein, Sarah Kaiser, Raman Kashyap, Matthieu Legre, Carter Minshull, and Shihan Sajeed. Laser damage creates backdoors in quantum communications. *arXiv:1510.03148 [quant-ph]*, October 2015.

[169] Shihan Sajeed, Igor Radchenko, Sarah Kaiser, Jean-Philippe Bourgoin, Anna Pappa, Laurent Monat, Matthieu Legré, and Vadim Makarov. Attacks exploiting deviation of mean photon number in quantum key distribution and coin tossing. *Phys. Rev. A*, 91(3):032326, March 2015.

[170] Feihu Xu, Kejin Wei, Shihan Sajeed, Sarah Kaiser, Shihai Sun, Zhiyuan Tang, Li Qian, Vadim Makarov, and Hoi-Kwong Lo. Experimental quantum key distribution with source flaws. *Phys. Rev. A*, 92(3):032305, September 2015.

[171] Raman Kashyap. The Fiber Fuse - from a curious effect to a critical issue: A 25$\hat{\text{t}}$h year retrospective. *Optics Express*, 21(5):6422, March 2013.

[172] Thorlabs, Inc. - Your Source for Fiber Optics, Laser Diodes, Optical Instrumentation and Polarization Measurement & Control. https://www.thorlabs.com/.

[173] Sarah Kaiser. Fiber fuse in optical splitter, June 2013.

[174] Bing Qi, Chi-Hang Fred Fung, Hoi-Kwong Lo, and Xiongfeng Ma. Time-shift Attack in Practical Quantum Cryptosystems. *Quantum Info. Comput.*, 7(1):73–82, January 2007.

[175] L. W. Tutt and T. F. Boggess. A review of optical limiting mechanisms and devices using organics, fullerenes, semiconductors and other materials. *Prog. Quant. Electr.*, 17:299–338, 1993.

[176] David Rideout, Thomas Jennewein, Giovanni Amelino-Camelia, Tommaso F. Demarie, Brendon L. Higgins, Achim Kempf, Adrian Kent, Raymond Laflamme, Xian Ma, Robert B. Mann, Eduardo Martín-Martínez, Nicolas C. Menicucci, John Moffat, Christoph Simon, Rafael Sorkin, Lee Smolin, and Daniel R. Terno. Fundamental quantum optics experiments conceivable with satellites—reaching relativistic distances and velocities. *Class. Quantum Grav.*, 29(22):224011, 2012.

[177] Daniel J. Bernstein, Johannes Buchmann, and Erik Dahmen, editors. *Post-Quantum Cryptography*. Springer Berlin Heidelberg, Berlin, Heidelberg, 2009.

[178] Christopher Gerry and Peter Knight. *Introductory Quantum Optics*. Cambridge University Press, 2005.

[179] Bruce Schneier. Wiley: Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd Edition. http://ca.wiley.com/WileyCDA/WileyTitle/productCd-0471117099.html.