Free Space Quantum Key Distribution to Moving Platforms

by

Christopher J. Pugh

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, 2017

EXAMINING COMMITTEE MEMBERSHIP

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

Supervisor: Dr. Thomas Jennewein, Associate Professor

Internal Member: Dr. Kevin Resch, Associate Professor

Internal Member: Dr. Robert Hill, Associate Professor

Internal-external Member: Dr. Michele Mosca, Professor

External Examiner: Dr. Dirk Englund, Associate Professor

AUTHOR'S DECLARATION

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

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

STATEMENT OF CONTRIBUTIONS

This thesis contains work done in collaboration with others but to which I made the major contribution. The contributions are listed below.

Chapter 1:

Chris Pugh wrote the introductory chapter.

Chapter 2:

Jean-François Lavigne, Brendon Higgins, and Chris Pugh wrote the code and performed the analysis.

Jean-Philippe Bourgoin and Thomas Jennewein provided background information and advice.

Chapter 3:

INO, Chris Pugh, Sarah Kaiser, Jean-Philippe Bourgoin, Brendon Higgins, and Thomas Jennewein designed the optical portion of the system.

INO built the optical portion of the system.

Neptec Design Group designed and built the control electronics portion of the system.

Sarah Kaiser and Jean-Philippe Bourgoin designed the mount between the telescope and the fine pointing unit.

Chris Pugh, Sarah Kaiser, Jean-Philippe Bourgoin and Isabelle Racicot performed the laboratory tests on the system.

Thomas Jennewein and Eric Choi, along with the Canadian Space Agency, managed the project.

Chapter 4:

Chris Pugh managed and led the airborne trials.

Sarah Kaiser, Chris Pugh, Brendon Higgins, and Thomas Jennewein conducted feasibility and aircraft flight-path studies, with link analysis conducted by Chris Pugh and Jean-Philippe Bourgoin.

Chris Pugh, Sarah Kaiser, Jean-Philippe Bourgoin, Brendon Higgins, and Thomas Jennewein designed and tested system components, with industry partners.

Ian D'Souza and Jeff Kehoe provided flight tests prior to collaboration with the NRC.

Phil Kaye provided a hangar at Smiths Falls–Montague Airport for storage of our equipment.

Thomas Jennewein conceived the study and supervised the project.

Chapter 5:

Chris Pugh, Eric Choi, and Thomas Jennewein managed the project, and planned and executed logistics.

Sarah Kaiser, Elena Anisimova, Vadim Makarov, and Thomas Jennewein designed and built the receiver detector module.

Chris Pugh and Sarah Kaiser designed and assembled the receiver payload.

Brendon Higgins developed the coarse pointing, data acquisition, data processing, and polarization compensation system software, supervised by Thomas Jennewein.

Jean-Philippe Bourgoin, Nigar Sultana, and Thomas Jennewein designed and built the quantum source.

Chris Pugh, Sarah Kaiser, Jean-Philippe Bourgoin, Jeongwan Jin, Sascha Agne, Brendon Higgins, and Thomas Jennewein conducted outdoor full-system calibration and tests.

Chris Pugh and Jeongwan Jin integrated the receiver payload into the aircraft, assisted by Brendon Higgins and the NRC FRL team.

Chris Pugh, Jean-Philippe Bourgoin, Brendon Higgins, and Thomas Jennewein developed and managed flight operations and mission tasking.

Chris Pugh operated the receiver in flight, assisted by Jeongwan Jin.

Brendon Higgins conducted data acquisition and pointing at the ground station.

Jean-Philippe Bourgoin operated the quantum source, assisted by Brendon Higgins.

Nigar Sultana, Sascha Agne, and Thomas Jennewein supported ground station operations.

Chapter 6:

Chris Pugh analyzed the data, supervised by Brendon Higgins and Thomas Jennewein.

Brendon Higgins modified the software for Time of Flight output.

Chris Pugh analyzed the output for the single photon ranging study, assisted by Thomas Jennewein.

Chapter 7:

Chris Pugh, Catherine Holloway, Jean-Philippe Bourgoin, Brendon Higgins performed the optics, pointing, link performance, beacon parameters, location calculations.

Cordell Grant, Chris Pugh, and Thomas Jennewein performed the radiator calculations.

Houman Hakima and Chris Pugh made the CAD drawings.

Chris Pugh and Eric Choi made the engineering budgets.

Thomas Jennewein conceived and supervised the project.

Chapter 8:

Chris Pugh wrote the concluding chapter.

ABSTRACT

The quantum space age has officially begun and many important milestones and achievements have recently been demonstrated, such as the exciting launch and results of the first quantum demonstration satellite, Micius. Previously with terrestrial applications, quantum key distribution was limited in distance to a few hundred kilometers through either free space or optical fiber. This had dampened progress towards a global quantum cryptographic network, but with the recent progress towards space implemented quantum systems, the door has been opened once again.

In this thesis, we begin by studying the effect of using an adaptive optics system to improve the efficiency of a free space link to a satellite for quantum key distribution. Adaptive optics has been used extensively in astronomy and has the potential to increase the average optical intensity received by the satellite. We study the effect of the atmosphere on the beam as it propagates from the ground station to the satellite. In the up-link configuration, the atmosphere is of special concern as it affects the beam at the beginning of the propagation, making the end effect worse.

One of the important components of a free space quantum key distribution satellite system is a fine pointing unit. We have, along with industry partners, designed and implemented such a unit for free space optical links. The device was designed to have little to no effect on the polarization of the photons used to transmit the key bits. The device was tested, both in the laboratory and outside and quantum key distribution was successfully performed while the fine pointing was active.

The main experiment of the thesis demonstrates quantum key distribution to a moving airplane from a ground station. The components of a quantum key distribution receiver prototype were tested locally around the University of Waterloo campus as well as some tests using private airplanes. The collaboration with the National Research Council of Canada really allowed the project to take flight by granting us access to a research aircraft to deploy our receiver prototype. This project spanned over three years and culminated in a two week flight campaign out of Ottawa and Smiths Falls Ontario.

Using only five flight hours we were able to successfully transmit finite size quantum secure keys from our optical ground station, located at Smiths Falls–Montague Airport

to a Twin Otter Research Aircraft housing our quantum key distribution receiver prototype. Many of the components implemented in the receiver were designed and built with spaceflight in mind and have a clear path to flight for space application.

Finally, we study the feasibility of implementing a quantum key distribution receiver onto a nano satellite. In partnership with the University of Toronto Institute for Aerospace Studies Space Flight Laboratory, we studied the various aspects such as optics, detection, cooling, power, mass, etc., to determine if it would be possible to perform quantum key distribution to a nano satellite. The main difference of this project from the previous Quantum Encryption and Science Satellite is the simpler pointing system, which doesn't utilize fine pointing.

Through various studies, experiments, and component design, we have shown the feasibility of implementing quantum key distribution to a moving aircraft in an up-link configuration. This work contributes to the long line of achievements leading towards satellite implementations of quantum key distribution for eventual global quantum cryptography.

ACKNOWLEDGEMENTS

To start, I would like to thank my supervisor Thomas Jennewein for giving me so many opportunities during this degree. I feel I have truly been given a great variety of experiences that I will think back on for many years to come. I would also like to thank my Advisory Committee members: Robert Hill, Michele Mosca, Kevin Resch, for the guidance and periodic check ins. I would also like to thank Dirk Englund for joining my Examining Committee. A special thank you to Dr. Brendon Higgins and Olivia Di Matteo for helping edit this document.

I would also like to thank all the Quantum Photonics Laboratory group members and collaborators, past and present, for all the discussions, fun, work, late nights, early mornings, and travel. The people you work with truly make the experience and you have made this one great for me. I won't list all the names here in case I miss any, but you all know who you are.

The Fun Office (Aimee Gunther and Ramy Tannous) made even the hardest days of coming into school worth it. So many shenanigans and so much fun happened in that office, for us and the IQC. Thank you for your willingness to put up with my craziness.

A huge thank you to all the members of the IQC, staff, faculty, post docs, and students for making my time here such an enjoyable experience. Also, thank you to the members of the UW community, many of whom I had the chance to work with on Senate, Board, and the GSA. I have learned so much through my experiences with this university that will help me throughout the rest of my life.

To the funding agencies that helped me accomplish this degree, I express sincere gratitude: NSERC Canadian Graduate Scholarship, Ontario Graduate Scholarship, and the University of Waterloo for my personal funding and CSA, NSERC, Ontario Ministry of Research and Innovation, CIFAR, FedDev Ontario, Industry Canada, CFI, and DRDC for the research funding.

To all the people who took me in as a son or brother (Matt and Patti Schumacher and family, John and Chris Dietrich, and the Knights of Columbus), thank you for making life outside of school enjoyable and for all the great times you have given me.

There is no way to express on paper the gratitude I have for all the love and support my family has offered me while pursuing this degree. I know the late night phone calls weren't always the easiest for you to answer, but thank you for listening to me when I needed it.

Lastly, and most of all, thank you to my Lord and God Jesus Christ for giving me the tools to accomplish what I have done. I look forward to what You have in store for me next.

DEDICATION

To William and Brenda Pugh, Breanna Hall, Jaime Pugh, Amanda Pilloud, Adelaide Zenk, and Dorrine Pugh

Table of Contents

Examining Committee ii

Author's Declaration iii

Statement of Contributions iv

Abstract vii

Acknowledgments ix

Dedication xi

Table of Contents xii

List of Figures xvii

List of Tables xxi

List of Acronyms xxiii

1 Photons, Quantum Communication, and Free Space Links 1

1.1 Quantum Information with Photons 1

1.1.1 The Photon 1

1.1.2 States of Light 2

1.1.3 Photons as Qubits 4

1.1.4 Single Photon Sources 5

1.2 Quantum Key Distribution . . . 6
1.2.1 Physical Security . . . 6
1.2.2 BB84 . . . 7
1.2.3 Classical Post Processing . . . 10
1.2.4 Decoy State QKD . . . 12
1.2.5 Finite Size Effects . . . 14
1.3 Quantum Channels . . . 14
1.3.1 Optical Fiber . . . 15
1.3.2 Free Space . . . 15
1.3.3 Satellite Free Space Quantum Key Distribution . . . 15
1.3.4 Transmission Losses in Free Space . . . 16
1.4 Conclusion . . . 19

2 Adaptive Optics for Quantum Key Distribution between an Earth station and a Satellite 20

2.1 Introduction . . . 20
2.2 Atmospheric and Orbital Model . . . 21
2.2.1 Atmospheric Effect on Beam Width . . . 25
2.3 Beam Wander Correction . . . 28
2.4 Higher Order Phase Corrections . . . 32
2.5 Adaptive Optics Analysis . . . 35
2.6 Discussion . . . 41
2.7 Conclusion . . . 42

3 A Fine Pointing System Suitable for Quantum Communications on a Satellite 43

3.1 Introduction . . . 43
3.2 Requirements . . . 44
3.3 Design . . . 50

3.3.1 Optical Portion . . . 50
3.3.2 Control Portion . . . 52
3.4 Performance . . . 53
3.4.1 Phase 1 . . . 55
3.4.2 Phase 2 . . . 55
3.4.3 Phase 3 . . . 61
3.4.4 Phase 4 . . . 62
3.5 Discussion . . . 76
3.6 Conclusion . . . 77

4 Preparation for Airborne Tests of Quantum Key Distribution 79
4.1 Introduction . . . 79
4.2 Project Management . . . 80
4.3 Feasibility and Requirements . . . 82
4.4 Preliminary Tests . . . 88
4.5 Flight Planning . . . 94
4.6 Discussion . . . 97

5 Experimental Airborne Tests of Quantum Key Distribution 99
5.1 Experimental Setup . . . 99
5.1.1 Source and Transmitter . . . 101
5.1.2 Receiver . . . 105
5.1.3 Acquisition and Calibration . . . 111
5.2 Experiment . . . 112

6 Airborne Quantum Key Distribution Results and Analysis 121
6.1 Analysis and Results . . . 121
6.1.1 Physical Performance . . . 122
6.1.2 Data Analysis . . . 133

6.2 Aside: Feasibility of Single-Photon Ranging . . . 136
6.2.1 Data Collection . . . 137
6.2.2 Analysis . . . 138
6.3 Discussion . . . 146
6.4 Conclusion . . . 147

7 The NanoQEY Mission: Ground to Space Quantum Key Distribution Using a Nanosatellite 148

7.1 Introduction . . . 148
7.2 Payload Design . . . 149
7.2.1 Optical Components . . . 153
7.2.2 Detection . . . 159
7.2.3 Data Processing . . . 165
7.2.4 Payload Assembly . . . 167
7.3 Pointing and Ground Station Location . . . 169
7.3.1 Constant Rate Tracking . . . 169
7.3.2 Beacon Laser . . . 170
7.3.3 Location . . . 172
7.4 Predicted Performance . . . 175
7.5 Engineering Budgets . . . 177
7.6 Schedule . . . 180
7.7 Discussion . . . 181
7.8 Conclusion . . . 182

8 Conclusion and Outlook 183

References 186

A Code for Adaptive Optics Effect on QKD 203

B Waypoint Calculators 226

C Selected Photos of Airborne Experiment **228**

D Publications and Media Attention **241**

D.1 Publications during PhD, 2013–2017 241

D.2 Conference Proceedings 241

D.3 Manuscripts in Preparation 242

D.4 Media Coverage 242

List of Figures

2.1 Structure function profiles 23
2.2 Bufton wind profiles 24
2.3 Impact of turbulence on beam 27
2.4 Tilt errors for various transmitter diameters 31
2.5 Strehl ratio and link efficiency for different wavelengths for number of modes fit 34
2.6 Link efficiencies for various atmospheric profiles with AO correction 37
2.7 Link Efficiency for a 400 km orbit with AO 38
2.8 Effect of different transmitter diameters on link efficiency 39
2.9 Link Efficiency using a laser guide star 18 km 40
2.10 Link Efficiency using a laser guide star at 30 km 40
2.11 Link Efficiency using a geostationary satellite 41

3.1 Reflectivity effect on visibility 47
3.2 Phase effect on visibility 48
3.3 Beacon loss through the atmosphere 49
3.4 FPU theoretical design 50
3.5 FPU optical design 51
3.6 Fine pointing unit 53
3.7 FPU mounted onto the telescope 54
3.8 Phase 2 FPU characterization setup 56
3.9 Polarization effect of the FPU 58

3.10 Polarized transmission over the field of view 60
3.11 QKD statistics for various mirror positions 63
3.12 Beacon power over time as measured on the QD 64
3.13 Sample x and y errors on the QD 65
3.14 One shot movements recorded by VN-300 70
3.15 One shot movements recorded by FPU 71
3.16 Angular speed of one movement of the motors in the y-direction. 72
3.17 Position of one-shot movement recorded by FPU 72
3.18 Count rate during one-shot movements 73
3.19 Count rate during one-shot movements zoomed in 74
3.20 Beacon power over slowly varying fluctuation 75
3.21 Spot error over time with a slowly varying beacon power 75
3.22 Count rate while the beacon power is varying slowly 76

4.1 Acceptable distances and altitudes for various angles of the telescope . . . 84
4.2 Fitting telescope into the helicopter and airplane 85
4.4 Beechcraft Bonanza airplane with WiFi antenna 89
4.5 WiFi connection times and distances 89
4.6 Receiver mounted in the Beechcraft Bonanza Airplane 90
4.7 Local tests of the equipment 91
4.8 FPU performance during stationary truck test 92
4.9 FPU performance while the truck was driving 93
4.10 Smiths Falls–Montague Airport from the airplane 95

5.1 Photo of the optical ground station 100
5.2 Schematic of the source 102
5.3 Transmitter breadboard 103
5.4 Network map of QKD equipment 104
5.5 Beacon laser assembly 105

5.6 Schematic of the receiver . . . 106
5.7 Integrated optical assembly, detector module and control and data processing unit . . . 107
5.8 Photo of the receiver mounted in the airplane . . . 109
5.9 Electronics and cables mounted in the airplane . . . 110
5.10 Collinearity measurement apparatus . . . 112
5.11 Flight paths on first night . . . 114
5.12 Flight paths on second night . . . 115
5.13 Flight paths on second night . . . 116

6.1 Airplane flight parameters for a 3 km arc . . . 123
6.2 Data from 5 km arc and 7 km line from the first night . . . 127
6.3 Data from 5 km arc and 3 km line from the second night . . . 128
6.4 Data from 3 km arc and 7 km arc from the second night . . . 129
6.5 Data from 10 km arc from the second night . . . 130
6.6 3 km arc fine pointing performance . . . 131
6.7 10 km arc fine pointing performance . . . 132
6.8 Screen-shot of the QKD software . . . 134
6.9 Description of time of flight . . . 137
6.10 GPS time of flight information . . . 138
6.11 One second chunk of time of flight information from photons . . . 139
6.12 Smaller time window view of photon time of flight . . . 140
6.13 Different bin sizes for photon time of flight for 10 km arc . . . 141
6.14 Different bin sizes for photon time of flight for 3 km arc . . . 142
6.15 Histogram of photon time of flight . . . 143
6.16 Relation between QBER and signal counts . . . 144
6.17 Low count rate drop in QBER . . . 145

7.1 NanoQEY block diagram . . . 150

7.2 NanoQEY payload volume . . . 152
7.3 Galilean beam expanders with 150 mm diameter . . . 154
7.4 Telescope optics weight . . . 155
7.5 Spot images for 150 mm Galilean telescope . . . 156
7.6 Clipping of rays vs. the input angle . . . 157
7.7 Passive QKD polarization analyzer . . . 158
7.8 Anode sensitivity temperature coefficient vs wavelength for PMTs . . . 159
7.9 Anode dark current vs. temperature for PMTs . . . 160
7.10 Dimensions of the H7422-40 detector . . . 161
7.11 Photocathode sensitivity vs. wavelength for the H7422 PMTs . . . 162
7.12 Atmospheric transmission . . . 163
7.13 Detector temperature vs. radiator size . . . 165
7.14 Schematic of the data acquisition device . . . 166
7.15 CAD models of NanoQEY . . . 168
7.16 Two dimensional constant rate tracking . . . 170
7.17 Beacon configuration . . . 171
7.18 Received beacon power . . . 171
7.19 Beacon loss with turbulence effects . . . 172
7.20 Background 45 km from Ottawa . . . 173
7.21 Background at Tenerife . . . 174
7.22 Background at Algonquin park . . . 175
7.23 Possible time line for NanoQEY mission . . . 181

List of Tables

1.1 Bit value assignments 8
1.2 BB84 quantum exchange scenario 9

2.1 Parameters for the HV models 23
2.2 Parameters for Bufton wind model 24
2.3 Parameters for AO study 26
2.4 Tilt error due to closed loop delay 29
2.5 Closed loop delay wavefront error in radians for different correction bandwidths 33

3.1 Requirements for a fine pointing unit 45
3.2 Polarization input and output expectations 57
3.3 Polarization input and output results for center of field of view 57
3.4 Position index 59
3.5 Collinearity measurement between quantum signal and beacon signal . . . 61
3.6 Mean spot error on QD for various movement and beacon fluctuations . . . 66
3.7 Standard deviation of the error on the QD for various movement and beacon fluctuations 67
3.8 QBER for various active tracking scenarios 68
3.9 Average count rate for various active tracking scenarios 68
3.10 Predicted secure key lengths for various active tracking scenarios 69

4.1 Timeline of airborne project 81
4.2 Angular rates of the aircraft 83

4.3 Telescope angles for various flight distances 83
4.4 Advantages and disadvantages between the helicopter and the airplane . . 87
4.5 WiFi distances and connection times 88
4.6 Flight types 96

5.1 Flights accomplished 113
5.2 Temperature data during flight campaign 118
5.3 Precipitation and wind data during flight campaign 119

6.1 Successful passes 122
6.2 Data from passes in the first night 124
6.3 Data from passes in the second night 125

7.1 Simplified NanoQEY requirements 151
7.2 Hamamatsu H7422 detector parameters 161
7.3 Parameters to calculate radiator cooling ability 164
7.4 Communication requirements for NanoQEY 167
7.5 Predicted key generation performance 176
7.6 Predicted usability 177
7.7 Power estimates for NanoQEY 178
7.8 Mass estimates for NanoQEY 179
7.9 Total mass 180

List of Acronyms

A: anti-diagonal polarization

AO: adaptive optics

AWG: arbitrary waveform generator

BB84: Bennett-Brassard 1984 quantum key distribution protocol

BBM92: Bennett-Brassard-Mermin 1992 quantum key distribution protocol

BC: beacon camera

BLA: beacon laser assembly

BLS: beacon laser source

CDPU: control and data processing unit

CDR: clock drift ratio

CPU: central processing unit

CSA: Canadian Space Agency

CW: continuous wave

CYSH: Smiths Falls-Montague Airport

D: diagonal polarization

DA×: diagonal/anti-diagonal or +/- basis

DAQ: data acquisition

DM: detector module

EDT: eastern daylight time

EPR: Einstein-Podolsky-Rosen

F: band-pass filter

FAST: Flights for the Advancement of Science and Technology grant

FPGA: field programmable gate array

FPC: fine pointing controller

FPU: fine pointing unit

FRL: Flight Research Laboratory

FSM: fast-steering mirror

FWHM: full-width-at-half-maximum

GPS: global positioning system

GUI: graphical user interface

H: horizontal polarization

HV: Hufnagel-Valley atmospheric model

HV+: horizontal/vertical or rectilinear basis

IM: intensity modulator

INMs: inertial navigation modules

IOA: integrated optical assembly

IQC: Institute for Quantum Computing

IRL: infra-red light-emitting diode array

L: left circular polarization

L1: 1590 nm continuous-wave laser

L2: 1550 nm triggered-pulsing laser

LDPC: low density parity check

LEO: low Earth orbit

LGS: laser guide star

LiDAR: Light, Detection, and Ranging

NanoQEY: Nano Quantum Encryption satellite

NEMO: Nanosatellite for Earth monitoring and Observation

NOTAM: Notice to Airmen

NRC: National Research Council of Canada

OA: optical attenuator

OCXO: oven-controlled crystal oscillator

OGS: optical ground station

OBC: on board computer

PBS: polarizing beam splitter

PC: personal computer

PMs: phase modulators

PMTs: photomultiplier tubes

PPMgO: periodically poled magnesium oxide

PPS: pulse per second

PSF: point-spread-function

PT: polarization tomography

QEYSSAT: Quantum Encryption and Science Satellite

QBER: quantum bit error rate

QD: quadrant detector

QKD: quantum key distribution

QKDR: quantum key distribution receiver

QPL: Quantum Photonics Laboratory

R: right circular polarization

RAC: Research Advancement Center

RAM: random access memory

RF: radio frequency

RL$\circ$: circular basis

RMS: root-mean-square

SFL: Space Flight Laboratory

Si-APD(s): silicon avalanche photodiode

SNR: signal-to-noise ratio

TT: time tagger

USB: universal serial bus

UTC: universal time coordinated

UTIAS: University of Toronto Institute for Aerospace Studies

UW: University of Waterloo

V: vertical polarization

WB: wide-field beacon

WCP: weak coherent pulse

WDM: wavelength division multiplexer

WiFi: classical radio frequency link

WPs: wave plates

XOR: sum modulo 2

YOW: Ottawa International Airport

Chapter 1

Photons, Quantum Communication, and Free Space Links

The purpose of this chapter is to introduce a few of the theoretical descriptions and ideas which will be used in the remainder of the thesis. The idea is not to give an in-depth explanation, but to allow the reader to have a basic understanding of the concepts.

1.1 Quantum Information with Photons

1.1.1 The Photon

A photon can be thought of as a quantized portion of the electromagnetic field, or a unit excitation of the electromagnetic field in a specific mode. In order to understand the photon sources described here, we will give a brief and simple description while more thorough descriptions can be found in many quantum optics texts [1–3]. To begin, following the derivation given in [2], we will utilize a particular solution to Maxwell's equations confined to a one dimensional cavity of length L along the z-axis, with the electric field polarized along the x-axis. This gives us electric and magnetic fields in a single mode

$$E_x(z,t) = \left(\frac{2\omega^2}{L\varepsilon_0}\right)^{1/2} q(t)\sin(kz), \tag{1.1}$$

$$B_y(z,t) = \left(\frac{\mu_0\varepsilon_0}{k}\right)\left(\frac{2\omega^2}{L\varepsilon_0}\right)^{1/2} \dot{q}(t)\cos(kz), \tag{1.2}$$

where ω is the frequency of the mode and k is the wave number. The wave is confined to the volume, V, and $q(t)$ is a time-dependent factor with dimensions of length. The

expressions $q(t)$ and $\dot{q}(t)$ appear as the canonical position and momentum respectively for a quantum harmonic oscillator ($\dot{q}(t) \to p(t)$) and which has unit mass. The field energy of this single mode, *i.e.* the Hamiltonian (with unit mass), H, is given by

$$H = \frac{1}{2}\int \mathrm{d}z \left[\varepsilon_0 E_x^2(z,t) + \frac{1}{\mu_0} B_y^2(z,t)\right]. \tag{1.3}$$

This Hamiltonian can be rewritten in the form of a quantum harmonic oscillator as

$$H = \frac{1}{2}(p^2 + \omega^2 q^2). \tag{1.4}$$

Now, using the correspondence rule, we replace the variables q and p with their operator equivalents, where $[\hat{q}, \hat{p}] = i\hbar$ ($\hat{q}$ and $\hat{p}$ are Hermitian, observable operators). It is now common to introduce non-Hermitian (non-observable) operators known as the annihilation ($\hat{a}$) and creation ($\hat{a}^\dagger$) operators

$$\hat{a} = (2\hbar\omega)^{-1/2}(\omega\hat{q} + i\hat{p}), \tag{1.5}$$

$$\hat{a}^\dagger = (2\hbar\omega)^{-1/2}(\omega\hat{q} - i\hat{p}). \tag{1.6}$$

These operators have the commutation relation $[\hat{a}, \hat{a}^\dagger] = 1$, and finally we write the Hamiltonian in Equation 1.4 as

$$\hat{H} = \hbar\omega\left(\hat{a}^\dagger\hat{a} + \frac{1}{2}\right). \tag{1.7}$$

The product of the annihilation and creation operators, $\hat{a}^\dagger\hat{a}$, is called the number operator, $\hat{n}$. Introducing the number state, $|n\rangle$, the number operator acts as $\hat{n}\,|n\rangle = n\,|n\rangle$. As a consequence, $|n\rangle$ is also an energy eigenstate of the single mode field that has the energy eigenvalue E_n:

$$\hat{H}\,|n\rangle = \hbar\omega\left(\hat{n} + \frac{1}{2}\right)|n\rangle = E_n\,|n\rangle\,. \tag{1.8}$$

Using the commutation relation between $\hat{a}$ and $\hat{a}^\dagger$, one can compute

$$\hat{H}\hat{a}\,|n\rangle = (E_n - \hbar\omega)\hat{a}\,|n\rangle\,, \tag{1.9}$$

$$\hat{H}\hat{a}^\dagger\,|n\rangle = (E_n + \hbar\omega)\hat{a}^\dagger\,|n\rangle\,. \tag{1.10}$$

From Equations 1.9 and 1.10 we can see that the annihilation and creation operators annihilate or create a *quantum* of energy, $\hbar\omega$, or rather unorthodoxly, a photon (this expression is not quite true, but for the simplicity of this explanation, we will use it).

1.1.2 States of Light

Two important states of light we will discuss are Fock states and coherent states.

1.1.2.1 Fock States

The ground state of the Hamiltonian in Equation 1.7 is defined as $|0\rangle$ where

$$\hat{a}\,|0\rangle = 0. \tag{1.11}$$

This $|0\rangle$ state is called the vacuum state and has zero photons present in the specific mode. When we act the creation operator on the vacuum state, we get

$$\hat{a}^\dagger\,|0\rangle = |1\rangle\,, \tag{1.12}$$

meaning that the operator has created a photon in this mode. Fock states, also known as number states, represent states that have a defined number of photons in a given mode. A state with n photons is represented as $|n\rangle$. Using the creation and annihilation operators and their energy relations, the action of the following operations can be derived

$$\hat{a}^\dagger\,|n\rangle = \sqrt{n+1}\,|n+1\rangle\,, \tag{1.13}$$

$$\hat{a}\,|n\rangle = \sqrt{n}\,|n-1\rangle\,, \tag{1.14}$$

$$\hat{n}\,|n\rangle = n\,|n\rangle\,, \tag{1.15}$$

where $\hat{n}$ is the previously defined number operator and is an observable measuring the number of photons in a given mode.

1.1.2.2 Coherent States

Another important type of state is the coherent state [4]. They are useful to help describe laser emission and are defined as

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_n \frac{\alpha^n}{\sqrt{n!}}\,|n\rangle\,, \tag{1.16}$$

where α is a complex number and the pre-factor fixes the normalization of the state. The Coherent state is an eigenstate of the annihilation operator:

$$\hat{a}\,|\alpha\rangle = \alpha\,|\alpha\rangle\,. \tag{1.17}$$

To calculate the mean photon number of a coherent state, one can compute the expectation value of the number operator to find

$$\langle\alpha|\,\hat{n}\,|\alpha\rangle = |\alpha|^2. \tag{1.18}$$

The number of photons in any given pulse is governed by Poissonian statistics.

A coherent state can also be generated by the displacement operator

$$D(\alpha) = \exp\left(\alpha\hat{a}^\dagger - \alpha^*\hat{a}\right), \tag{1.19}$$

operating on the vacuum state

$$D(\alpha)\,|0\rangle = |\alpha\rangle\,. \tag{1.20}$$

In order to see the above, it is best to rewrite Equation 1.19 using Glauber's identity

$$D(\alpha) = e^{-\frac{1}{2}|\alpha|^2} e^{\alpha\hat{a}^\dagger} e^{-\alpha^*\hat{a}}, \tag{1.21}$$

from which we can see

$$\begin{aligned} D(\alpha)\,|0\rangle &= e^{-\frac{1}{2}|\alpha|^2} e^{\alpha\hat{a}^\dagger} \sum_n \frac{(-\alpha^*)^n}{n!}\hat{a}^n\,|0\rangle\,, & (1.22)\\ &= e^{-\frac{1}{2}|\alpha|^2} \sum_n \frac{\alpha^n}{n!}\hat{a}^n\,|0\rangle\,, & (1.23)\\ &= e^{-\frac{1}{2}|\alpha|^2} \sum_n \frac{\alpha^n}{\sqrt{n!}}\,|n\rangle\,. & (1.24) \end{aligned}$$

This state will help us to describe our weak coherent pulse source (WCP) below.

1.1.3 Photons as Qubits

In order to perform the protocols described later on, we need a quantum bit or qubit, which is the quantum analog of a bit. A qubit is a two-state quantum mechanical system that, unlike a classical bit which can be either a 0 or a 1, can be in a superposition of 0 and 1 [5]

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,, \tag{1.25}$$

where α and β are complex numbers. The probability of measuring the state $|0\rangle$ is given by $|\alpha|^2$ and the state $|1\rangle$ by $|\beta|^2$ where $|\alpha|^2 + |\beta|^2 = 1$.

Photons offer many degrees of freedom, supplying two or more levels which can be considered as qubits, or qudits (d-dimensional systems). Some of these include polarization, time-bin [6], path [7], and orbital angular momentum [8].

The degree of freedom that we are interested in for this thesis is polarization for its simplicity and because the atmosphere is not birefringent for our wavelength. In order to implement the protocols described below, we require two, two-dimensional mutually unbiased bases[1] each consisting of two polarization states. The photon conveniently provides

[1]Mutually unbiased bases in two dimensions are two orthonormal bases where the square of the magnitude of the inner product between any two states, one from each basis, equals 1/2, $|\langle s_a|s_b\rangle|^2 = \frac{1}{2}$ [9].

this, and more. There are three mutually unbiased bases for photons the first of which being the rectilinear basis. The two states in this basis are the horizontal (H) and vertical (V) states [5]

$$|\rightarrow\rangle = |H\rangle \quad = \quad |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \tag{1.26}$$

$$|\uparrow\rangle = |V\rangle \quad = \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \tag{1.27}$$

written in ket and matrix notation. The next two bases consist of superpositions of these states. The second basis is the diagonal basis which consists of the diagonal (D) state and the anti-diagonal (A) state

$$|\nearrow\rangle = |D\rangle \quad = \quad \frac{|0\rangle + |1\rangle}{\sqrt{2}} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \tag{1.28}$$

$$|\searrow\rangle = |A\rangle \quad = \quad \frac{|0\rangle - |1\rangle}{\sqrt{2}} = \begin{pmatrix} 1 \\ -1 \end{pmatrix}. \tag{1.29}$$

The last basis is the circular basis which consists of left circularly- (L) and right circularly- (R) polarized photons

$$|L\rangle \quad = \quad \frac{|0\rangle + i\,|1\rangle}{\sqrt{2}} = \begin{pmatrix} 1 \\ i \end{pmatrix}, \tag{1.30}$$

$$|R\rangle \quad = \quad \frac{|0\rangle - i\,|1\rangle}{\sqrt{2}} = \begin{pmatrix} 1 \\ -i \end{pmatrix}. \tag{1.31}$$

When any of these states is measured in the same basis in which it was produced, it will yield the original state with certainty. When a state is measured in a different basis, however, there will be a 50 % chance of yielding either state in the measured basis with no correlation to the original state. This will be of fundamental importance for Quantum Key Distribution.

1.1.4 Single Photon Sources

The ideal single photon source would be able to emit a single photon with the desired characteristics on demand. Many device candidates are being studied to create single photons such as quantum dots, nitrogen-vacancy centers, photonic crystals yielding heralded photons, weak coherent pulses, and trapped atoms [10] (and the sources therein). Each

of these devices has their advantages and drawbacks, but for practical reasons one of the most common single photon sources used in QKD is the weak coherent pulse source.

This type of source is created by attenuating laser pulses, which contain many photons, so that the mean photon number per pulse is less than one. In practice, one typically will attenuate a coherent state, which follows a Poissonian distribution, meaning the lower the mean photon number, the more unlikely the higher photon number pulses become. The drawback is an increase in 0-photon pulses, therefore decreasing the signal of the source. Given a source with a mean photon number of μ, ($\mu = |\alpha|^2$), the probability distribution of having n photons in a pulse is given by [11]

$$p(n, \mu) = \frac{\mu^n e^{-\mu}}{n!}. \tag{1.32}$$

As an example, if $\mu = 0.1$ then the output state will be given as $\sqrt{0.905}\,|0\rangle + \sqrt{0.09}\,|1\rangle + \sqrt{0.002}\,|2\rangle + ...$ This means that if a pulse being attenuated does contain photons, there is a greater than 95 % probability it contains just a single photon[2]. The mean photon number can thus be manipulated to determine the single photon probability per pulse versus the percent chance a pulse has a photon.

1.2 Quantum Key Distribution

In 1984, Charles Bennett and Gilles Brassard introduced the first quantum cryptography protocol known as the BB84 protocol [12], referred to as Quantum Key Distribution (QKD). This was the first cryptographic protocol that moved from using unproven computational complexity security [13] to using fundamental laws of nature, quantum mechanics, to prove its security. Since this first proposal in 1984, there have been other protocols such as a two-state protocol [14], the six-state protocol [15, 16], the EPR protocol [17], and many more. BB84 will be the focus of this thesis.

1.2.1 Physical Security

Approximately a decade after the BB84 protocol was conceived, it was proven to be cryptanalytically secure [18–20]. The basis of the security of BB84 lies in the Heisenberg uncertainty principle [21] and in the no cloning theorem [22,23]. In simple terms, the Heisenberg

[2] $P(1|1 \text{ or more}) = \frac{P(1)}{P(1 \text{ or more})}$. From the Poissonian distribution we have $P(1) = e^{-\mu}\mu$ and $P(0) = e^{-\mu}$. We also know that $P(1 \text{ or more}) = 1 - P(0)$, therefore $P(1|1 \text{ or more}) = \frac{e^{-\mu}\mu}{1-e^{-\mu}}$ and with $\mu = 0.1$ we have $P(1|1 \text{ or more}) \approx 0.951$

uncertainty principle states that the more precisely one knows a particular aspect of a given state, the less precisely one knows some different aspect of a given state. This relation applies when the two aspects are complementary variables [24]. Most commonly, this is shown for position, x, and momentum, p, as

$$\sigma_x \sigma_p \geq \frac{\hbar}{2}. \tag{1.33}$$

This implies that the more precisely one knows about the momentum of a particle, the less precisely one knows about the position and vice-versa.

With regards to the no cloning theorem, let us say that there are two non-orthogonal quantum states given as $|\psi\rangle$ and $|\phi\rangle$. Assume that there is access to an ancilla bit, $|u\rangle$, and that unitary actions may be performed. Making the assumption that these actions do not disturb the state, one yields [5]

$$|\psi\rangle |u\rangle \rightarrow |\psi\rangle |v\rangle , \tag{1.34}$$

$$|\phi\rangle |u\rangle \rightarrow |\phi\rangle |v'\rangle . \tag{1.35}$$

In order to gain information on the system, $|v\rangle$ and $|v'\rangle$ must be different, but since inner products are preserved when states undergo unitary transformations it must be the case that

$$\langle v|v'\rangle \langle \psi|\phi\rangle = \langle u|u\rangle \langle \psi|\phi\rangle , \tag{1.36}$$

$$\langle v|v'\rangle = \langle u|u\rangle = 1, \tag{1.37}$$

which means that $|v\rangle$ and $|v'\rangle$ are identical. This means that one of the states $|\psi\rangle$ or $|\phi\rangle$ must be disturbed to distinguish between them.

The most common QKD protocols encode their information onto photons which are individual quanta of light and due to the no cloning theorem, cannot be reproduced. Different degrees of freedom of the photon provide the encoding platform for the information and will be discussed further below.

1.2.2 BB84

The BB84 protocol [12] is referred to as a *prepare and send* protocol since the states are prepared by one party, herein referred to as Alice, and received and measured by another party, herein referred to as Bob. This protocol, and the methods in this thesis, utilize the polarization degree of freedom of the photon, but other degrees such as time-bin [25, 26], phase [27, 28], frequency [29], and spatial modes [30], to name a few. Each of

Basis	0	1
+	→	↑
×	↗	↘

Table 1.1: The bit value assignments in the HV+ basis and in the DA× basis.

these degrees of freedom offer advantages and disadvantages depending on the propagation tool. For instance, the birefringence of fibers make the phase degree of freedom much more advantageous than the polarization degree. Since the atmosphere is not birefringent for our wavelength, it makes polarization a very useful choice.

To begin, Alice has the ability to generate photons in one of two non-orthogonal polarization bases, e.g. the Horizontal/Vertical (HV+) basis and the Diagonal/Anti-diagonal (DA×) basis. Each of these bases contains two states, H and V in the first, and D and A in the second (as per Section 1.1.3). Alice will, traditionally, encode the H and D state with a 0, and the V and A state with a 1 in binary format as shown in Table 1.1. With this method, each basis has both a 0 and a 1 bit which can be selected randomly. The reference frame for the polarization will be the lab frame.

Bob has a module that allows him to measure in either the HV+ basis or the DA× basis. If the measurement basis and the polarization type match, Bob is guaranteed to get the correct bit value that was sent by Alice. If Bob measures in the other basis, his result has a 50 % chance of being a 0 or a 1. Since the bases are mutually unbiased, measurement in the wrong basis yields no information about the original state.

The first step in this protocol is the quantum transmission portion. Alice will randomly generate a secret bit (0 or 1) string of length N (ideally generated with a quantum random number generator [31]). She will also randomly generate a secret string of basis choices of length N. Bob too will generate a random secret string of basis choices of length N.

Once these strings are created, Alice will prepare her single photons and send them over the quantum channel to Bob. Bob will measure each photon according to his pre-selected bases and record the value of the bit measured. They continue this procedure until all N photons have been sent across the quantum channel.

Upon completion of this task, Bob will publicly announce, over an authenticated classical channel, the basis in which he measured each photon (his random string of N basis choices) and Alice will confirm whether each choice matches the basis in which she created her photon. As the channel is public and classical, anyone can listen in, however, authentication guarantees Alice and Bob are speaking with each other and not, for example, a malicious eavesdropper. Alice and Bob will keep any bits where their bases matched (there

Alice's Bit	0	0	1	1	0	1	0	1	0	1
Alice's Basis	+	+	+	×	+	×	×	+	+	×
State Sent	↑	→	↑	↘	→	↘	↗	↑	→	↘
Bob's Measurement Basis	+	×	×	×	+	+	×	+	×	+
Bob's Result	↑	↗	↘	↘	→	↑	↗	↑	↗	→
Bob's Bit	1	0	1	1	0	1	0	1	0	0
Shared Secret Key	**1**	×	×	**1**	**0**	×	**0**	**1**	×	×

Table 1.2: Example of BB84: Alice generates a random bit string and chooses the equivalent amount of random bases. She then prepares her photons in the polarizations associated with those bits and bases and sends them to Bob. Bob measures each photon in one of the two measurement bases randomly and records the bit value. Bob then announces his measurement bases and they throw away any trials where the bases didn't match.

can still be some information gained from these other bits, but we will not discuss that here). An example for a few bits can be seen in Table 1.2. On average, they will keep about half of the bits that they send so the secret key at the end will be approximately of length $N/2$, or lower if transmission losses occur.

This is the end of the quantum portion of the protocol, and it leaves Alice and Bob with a *sifted key*. In a perfect world with perfect devices and no eavesdropper (commonly named Eve), this *sifted key* would be the same for both Alice and Bob. In reality, there is noise in the channel as well as the possibility of Eve interfering with the transmission meaning that their *sifted keys* may not be the same. The error rate in the transmission tends to be around a few percent, which is much greater than the 10^{-9} error rate which is common in classical optical communication. This error rate is known as the quantum bit error ratio (QBER) and is a very important metric. The QBER can be calculated as

$$QBER = \frac{N_i}{N_i + N_c}, \tag{1.38}$$

where N_i is the number of incorrect detections and N_c is the number of correct detections when comparing bits. If the visibility of the polarization, the encoding used for this protocol, is given as

$$V = \frac{N_c - N_i}{N_c + N_i}, \tag{1.39}$$

then the QBER can be related to this quantity for qubits by

$$QBER = \frac{1 - V}{2}. \tag{1.40}$$

Theoretically, the protocol can be proven secure against the influence of an eavesdropper if the QBER is less than 11 %. With practical systems this percent must drop, but many schemes can still tolerate a QBER of 3 % to 5 %, which also gives a bound on the visibility of the polarization.

The protocol then moves into the classical post-processing stage. Technically the basis sifting also falls under classical post-processing but it is common to describe it with the transmission. We defer discussion at this stage to Section 1.2.3.

At this point it is instructive to examine how one of the most basic attacks would affect the system; the intercept-resend attack. The basic principle behind this attack is Eve will take each qubit that Alice has sent and measure them exactly the same way Bob would have. She then sends a new qubit to Bob based on her measurement outcome. In approximately half the cases, Eve will measure in the correct basis, get the correct measurement result and forward the correct qubit to Bob. In this case, Alice and Bob will not notice any influence from Eve as she has forwarded the same state which Alice originally sent. In the other half of cases, however, Eve will measure in the wrong basis and prepare a qubit with only $\frac{1}{2}$ overlap with the correct states. This means Alice and Bob will measure errors in half of these cases as their results are now randomly correlated.

When Eve uses this attack, she will get 50 % of the information but Alice and Bob will have approximately a 25 % QBER once they remove the cases where their bases didn't match. This QBER easily demonstrates to them that there was an eavesdropper interfering with their channel. We will discuss a more complex attack in upcoming sections.

1.2.3 Classical Post Processing

As mentioned in the previous section, due to noise and the possibility of Eve manipulating the transmission, the *sifted keys* will most likely have errors or differences between Alice's version and Bob's version. The next step in the protocol is known as error correction. We begin by examining a very simple case following the example given by [32].

Assume that we have a joint probability distribution given by $P(\alpha, \beta, \epsilon)$ between the three parties. Alice and Bob can determine the marginal distribution given by $P(\alpha, \beta)$ and from this and their knowledge of quantum mechanics, must try to find information about $P(\alpha, \beta, \epsilon)$, which will help them determine the amount of information Eve has about their shared key. As this distribution is currently not known, the conditions for a positive secret key rate between Alice and Bob, $S(\alpha, \beta||\epsilon)$, is also not known. A useful way to determine a lower bound can be given by the difference between Alice and Bob's mutual Shannon

information, $I(\alpha, \beta)$ and Eve's mutual information [33]

$$S(\alpha, \beta||\epsilon) \geq \max[I(\alpha, \beta) - I(\alpha, \epsilon), I(\alpha, \beta) - I(\beta, \epsilon)]. \tag{1.41}$$

This implies that when Bob has more information than Eve about Alice's key, a secure key can be distilled [34].

A simple example of how to determine if a key can be generated is to first estimate the QBER in the key. This can be done by Alice and Bob randomly revealing a subset of their bits and determining the differences. This will give them an idea of the error rate (which relates to $P(\alpha, \beta)$) in the entire key and they can discern the amount of information known to Eve. If they determine Eve has too much information, they simply do not use the generated key and restart the protocol. If a key can be distilled, they proceed to error correction after discarding the bits they revealed.

A simple version of error correction can be achieved by Alice randomly choosing pairs of bits and announcing their XOR (sum modulo 2) to Bob. If Bob's XOR agrees with Alice's, they accept and if they are different, they reject. If the pair is accepted, they both keep the first bit of the pair and discard the second bit. If the pair is rejected, they discard both bits.

The simple model above is just an example of an algorithm, but in practice other more efficient and complex algorithms are used. Two of the most common forms of Error Correction are the CASCADE [35] and Low Density Parity Check (LDPC) [4, 36–38] algorithms. These codes, similar to the example above, check the parities between blocks of Alice's and Bob's sifted keys, but use larger blocks, binary search algorithms and other more complex techniques to improve the efficiency. After this stage is finished, Alice and Bob now share a secret key (with high probability), known as an *error corrected key*.

At this point, Eve still can have information about the *error corrected key* and thus Alice and Bob must perform one more step to ensure the security of their key. This step, known as privacy amplification, will reduce the size of their key depending on how much information they estimate Eve to have. A very simple method of privacy amplification has Alice pick two bits and XOR them and announce to Bob which bits she chose, but not the XOR value. He then performs the same operation on the same bits and they continue this way, keeping the XOR values, until they have reduced their key to a secure length. A more complex, and more common way to perform Privacy Amplification for QKD is to use universal hash functions [39].

After this step, Alice and Bob finally share a secret key. This key, when used in a symetric key algorithm, such as the One-Time-Pad [40] is guaranteed to be secure. Of

course there still are some practical issues that can be taken into account [41], but these issues are beyond the scope of this discussion.

1.2.4 Decoy State QKD

One important aspect to take into consideration when discussing QKD is the practical devices used to implement the protocol. These devices, such as detectors, sources, quantum channels etc. have imperfections that will lead to errors and possibly openings for attacks. One such attack, the photon-number-splitting attack, and its countermeasure will be discussed. Many other attacks have been studied, some of which can be found in [32, 42, 43].

In modern single photon sources, it is never assured that they are producing precisely single photons. Every pulse has the possibility of emitting 0, 1, 2 or more photons which can open the QKD system up to a photon-number-splitting attack [44]. In this attack, Eve deterministically separates off one photon in each multi-photon pulse, using a quantum non demolition measurement, stores it, and sends the rest of the photons in that pulse to Bob. Once Bob makes his measurements and announces his bases to Alice, Eve will measure her stored photons in the same basis as Bob. When Eve can replace the lossy channel with a noiseless channel, she can actively suppresses the single photon pulses, preventing them from reaching Bob and can mimic the results Bob would expect in the lossy channel and remain undetected. This attack allows Eve to gather all the information about the secure key without Alice and Bob knowing. Clearly this is cause for concern due to limitations of modern photon sources.

In 2003, a protocol was proposed by Hwang [45], and further developed by Lo, Ma and Chen [46], to combat the issue of multi-photon emissions. This protocol was named the decoy state QKD protocol. To begin the analysis of this protocol, first we introduce the secure key generation rate per signal state emitted by Alice as [42]:

$$r \geq Q_\mu\{-H_2(\mathrm{QBER}_\mu) + \Omega[1 - H_2(e_1)]\}, \tag{1.42}$$

where

- Q_μ is the gain of the signal state,
- QBER_μ is the QBER of the signal state,
- Ω is the fraction of detection events by Bob that came from single-photon signals from Alice,

- e_1 is the QBER of the detections at Bob that were from single-photon signals from Alice,
- and H_2 is the binary Shannon Entropy, $H_2(p) = -p\log_2(p) - (1-p)\log_2(1-p)$.

Gottesman *et al.* [42] make worst case assumptions on the lower bound of Ω and the upper bound on e_1 which generally reduces QKD system performance (maximum achievable distance) in order to maintain unconditional security.

The protocol that Lo *et al.* implement demonstrates a reasonable way to determine the bounds that were previously challenging to obtain, those on Ω and e_1. The idea here is that Alice will prepare and send decoy states in addition to the standard BB84 states interspersed in the sequence. These states will only be used to detect the presence of an eavesdropper and will not be used to generate key. The only difference between the decoy states and the signal states is the intensity of the pulses. In theory, an infinite number of decoy states ensure security, but it has been shown that only a few states can also work, for example, a vacuum state (μ=0), a weak decoy state ($\mu << 1$), and a signal state ($\mu = O(1)$) [47].

The essence of the decoy state protocol is that Eve cannot distinguish between a signal state and a decoy state since they are identical except for intensity. The only thing Eve is able to determine is the number of photons in the pulses. When Eve is selectively blocking pulses that have only single photons she will remove more often decoy pulses than signal pulses. This will create a discrepancy in the yields and QBER of the decoy states vs. the signal states and Alice and Bob can detect this difference and determine that there is an eavesdropper.

As in the analysis in [46], with implications from practical error correction protocols, the new key generation rate is given by

$$r \geq q\{-Q_\mu f(E_\mu)H_2(E_\mu) + Q_1[1 - H_2(e_1)]\}, \tag{1.43}$$

where q depends on which QKD protocol is used (1/2 for BB84 due to the fact that half the time the measurement is in the wrong basis), $f(E_\mu)$ is the error correction efficiency [35], and Q_1 is the gain for the single-photon state. Measuring the yields and QBER of the decoy states allow one to compute a better measure on Q_1 as well as e_1 yielding a higher key generation rate while maintaining security [46]. This is a very important protocol for realistic implementations and was demonstrated for the first time in [48].

1.2.5 Finite Size Effects

Many of the assumptions made above for secret key generation assume an infinite key length and an infinite amount of decoy states, which is of course not practically feasible. Studies on the effects of statistical fluctuations have been done to determine the secure key rates when we no longer assume infinite key or states [49–52]. These fluctuations may arise due to a number of reasons such as the intensity of the laser, the Poissonian output of photons from the imperfect source, the yields of the signal state vs. the decoy states, and others [47].

The yield and QBER of the single photon pulse from Equation 1.43 (as described in [46]) can be recalculated to take into account the statistical fluctuations of the gain and QBER parameters for various photon numbers, as shown in [52]. If each parameter is estimated within 10 standard deviations (10 σ) the statistical fluctuation in the secure key rate will be less than 10^{-25}. The final key rate can be calculated by [52]

$$r = q(n/N)\{Q_1[1 - H_2(e_1) - \Delta_1] - \Delta_2/n - Q_\mu 1.22 H_2(E_\mu)\}, \tag{1.44}$$

where N is the total number of transmitted pulses, n is the number of pulses chosen for the raw key by Alice, μ is the intensity of the signal states, and [51]

$$\Delta_1 = 7\sqrt{\log_2(2/(\bar{\varepsilon} - \bar{\varepsilon}'))/nQ_1}, \tag{1.45}$$

$$\Delta_2 = 2\log_2(1/2(\varepsilon - \bar{\varepsilon} - \varepsilon_{\mathrm{EC}})). \tag{1.46}$$

Equations 1.45 and 1.46 are the security parameters for error correction and privacy amplification where ε is the security bound, $\varepsilon_{\mathrm{EC}}$ is the error probability of error correction, and $\bar{\varepsilon}$ and $\bar{\varepsilon}'$ are parameters used to optimize the key rate.

The rate formula in Equation 1.44 can be used to estimate the non-asymptotic or finite-size affected key rate for a decoy state protocol. Since all practical systems involve these statistical fluctuations in their implementation, this is a more realistic approach to calculating the key rate as compared to Equation 1.43.

1.3 Quantum Channels

Optical communications, including QKD, tend to be implemented using two types of channel media, optical fibers and free space. These channels allow for the propagation of photons from Alice to Bob for generation of the secure key.

1.3.1 Optical Fiber

Optical fiber can be used to transmit the single photon states for QKD from Alice to Bob. Many successful demonstrations have been shown using optical fibers (a small selection being [53–57]) and they have even been implemented in full networks [58–61]. Ground based implementations of QKD using optical fiber links are limited to distances of a few hundred kilometers due to absorption losses, which scale exponentially with distance, leading to insufficient signal-to-noise ratios [57, 62, 63]. The fibers are also generally birefringent which will cause many problems for polarization encoded schemes and thus fiber generally favors phase or time-bin schemes.

The benefit of this method is that large scale fiber networks are already in place due to the classical telecommunications industry. The QKD signal can be inserted into the active fibers [64–66] and therefore reduce the cost of installing new infrastructure. This solution would be beneficial at a municipal level to create a network within a city or organization, but there is still the problem of reaching longer distances. This will be addressed with free space links.

1.3.2 Free Space

Free space optical channels consist of a transmitter sending the quantum signals from Alice to a receiver at Bob located some distance away through open air. The scaling of loss with distance in a free space channel is quadratic [67], as opposed to exponential in fiber [68], which is very enticing for long-distance applications. Despite this, the addition of atmospheric absorption and turbulence, and the necessity of having clear line of sight also limits terrestrial free-space transmissions to a few hundred kilometers. The first demonstration of QKD over free space was achieved by Bennett *et al.* in 1991 [34] and has increased in distance up to 144 km in stationary configurations [69–73] and moving [74–76] configurations. As this is the main focus of this thesis, this will be discussed in more detail in the following sections and chapters.

1.3.3 Satellite Free Space Quantum Key Distribution

Much greater distances could be spanned in free-space transmissions outside Earth's atmosphere. Utilizing orbiting satellites therefore has potential to allow the establishment of global QKD networks, with these satellites acting as intermediaries. Such satellites could operate as untrusted nodes linking two ground stations simultaneously [77, 78], or trusted

nodes connecting any two ground stations on Earth at different times [79–87]. The majority of such analyses propose a quantum downlink, where photons are generated at the satellite and transmitted to receivers on the ground. The proposed QEYSSat [88,89] concept, in contrast to many other missions, proposes a quantum uplink, placing the receiver (Bob) on the satellite while keeping the quantum source (Alice) at the ground station.

Under similar conditions, the uplink configuration has a lower key generation rate than the downlink, due to the atmospheric turbulence affecting the beam path at the beginning of the propagation, however, this decrease has been shown to only be of one order of magnitude [89]. Implementing an uplink has a few key advantages over the downlink configuration such as the relative simplicity of the satellite design (less demanding processing and storage requirements, passive photon analysis), and the flexibility of being able to use various different quantum source types with the same receiver apparatus. Although, advances in quantum sources have been made and are showing promising and space suitable results [90–92]. Recently, China launched a quantum science satellite which aims to perform many quantum experiments with optical links between space and ground [93,94], the first of which was entanglement distribution at distances over 1200 km [95], and the following two were demonstrations of teleportation [96] and QKD [97].

1.3.4 Transmission Losses in Free Space

As optical beams pass through the atmosphere they experience loss due to many different factors: diffraction, atmospheric absorption and scattering, pointing error; there is further more the issue of equipment losses. These will be described in detail in this section.

1.3.4.1 Diffraction

A Gaussian beam in free space will have some minimum beam waist (radius) given as W_0. This waist is measured with resepect to the position where the beam intensity reaches a level of $1/e^2 \approx 13.5\%$ of the on-axis intensity. The beam will naturally diffract when propagating through free space given by [68]

$$W(z) = W_0\sqrt{1+\left(\frac{z}{z_0}\right)^2}, \tag{1.47}$$

where z is the propagation distance from the minimum beam waist and z_0 is the Rayleigh range

$$z_0 = \frac{W_0^2\pi}{\lambda}, \tag{1.48}$$

where λ is the wavelength of the light. This is the minimum beam divergence as a function of propagation distance that one can achieve through free space propagation even when the beam is collimated. This is known as the diffraction limit. The waist radius, W_0, for our applications is proportional to the diameter of the transmitter telescope. This means that even if there were no other factors, such as those described below, the beam would still grow in size and induce loss due to the finite size of the receiver.

For distances $z >> z_0$, the first term in Equation 1.47 becomes negligible and the radius of the beam can be estimated as $W(z) \approx \frac{W_0}{z_0} z$. By setting $W_0/z_0 = \theta_0$ it is seen that the beam diverges in a cone with half angle θ_0 related to the minimum beam waist and the wavelength.

1.3.4.2 Atmospheric Turbulence

Natural small eddies, or temperature differences, in the atmosphere at differing scales cause changes in the density of the air mass which light is propagating through. These changing densities mean the refractive index of the various pockets will vary and cause the beam to experience different effects in different areas. These eddies will cause multiple effects to the beam such as scintillation, beam wander and beam broadening [98]. Scintillation consists of intensity fluctuations across the beam, and is mainly a factor when the beam is larger than the different pockets of air it is traveling through; physically it can be seen as a shimmer in the beam. Scintillation can have a negative effect on the quality of images one can achieve when observing through the atmosphere. For the purpose of collecting light, as in the QKD application, this factor is less important as it is the average intensity that generates key, not the short term intensity. This arises as only the photons that are actually measured by Bob are included in the raw key.

The beam wander, also called tilt, can cause pointing errors in the beam when trying to target an object. The beam will be moved around and deflected, which occurs often when the beam is smaller than the pockets of air in which it is propagating. This effect can be seen on a shorter term time scale as the beam will dance around the central propagation direction at different rates depending on the strength of the turbulence.

The last effect we consider is beam broadening, which can occur through higher order phase errors inflicted on the beam. A few of these effects are commonly known, such as astigmatism and coma, and have similar analogies in analysis of the eye. These effects cause the beam to grow faster than the rate of diffraction and induce more loss in the propagation due to the increased size of the beam relative to the receiver telescope.

Two important parameters for modeling atmospheric turbulence are the refractive-index structure constant C_n^2 and Fried's coherence length, r_0 [98]. The refractive-index structure constant is a measure of the strength of the turbulence which varies for different locations and altitudes and during different weather patterns. Different models [99–102] have been developed, and measurements [103, 104] have been taken for the purpose of modeling this phenomenon but due to its complexity, no model perfectly matches the data. One of the most common models is the Hufnagel-Valley (HV) model which will be detailed in Chapter 2.

Fried's coherence length [105] defines the maximum allowable diameter of a collector or telescope before atmospheric turbulence dominates the performance of the link. This measure is commonly on the order of centimeters and can be 20 cm or above for sites with great atmospheric quality.

1.3.4.3 Atmospheric Transmission

The atmosphere is composed of many constituent chemicals which can cause both absorption of light as well as scattering [106]. Absorption will depend on the types of chemicals such as N_2, CO_2, water vapor and others and will severely hamper certain wavelengths from transmitting great distances.

Scattering occurs mainly due to two effects, Rayleigh and Mie scattering [106, 107]. Rayleigh scattering is caused by the scattering of light off particles which are much smaller than the wavelength of the light. This is the reason for the blue color of the sky, as this type of scattering affects lower wavelengths more strongly. Mie scattering is caused by larger particles in the air, on the order of the wavelength of light.

1.3.4.4 Pointing Error

A number of applications have been studied which require pointing telescopes between two objects to create an optical link. This problem has numerous solutions and is used in many satellite technologies currently as well as ground-based applications. For the purpose of pointing the beam of photons at a satellite, as in the uplink configuration, the ground station will need precise pointing in order to correctly target the satellite for QKD. The errors from pointing can be averaged over time and be considered as a long-term beam broadening [108]. This too, will act as if the size of the beam has increased and cause more loss.

By having a larger field of view and aperture on the satellite, the pointing requirements are relaxed for this platform which reduces complexity. The pointing at the ground station, however, must be very precise and the majority of the loss due to pointing errors comes from the ground station pointing error.

1.3.4.5 Equipment Losses

This loss factor comes from the inefficiencies of the equipment itself in terms of absorption and scattering. The signal must travel from the source to the detectors by passing through lenses, mirrors, telescopes, beam splitters, and potentially fibers. Each of these items has some loss factor which will decrease the total amount of signal.

Another factor which falls in this category is the efficiency of the detectors. These devices range in efficiency with some achieving as high as >90 % [109]. These efficiencies depend on the technology which ranges from photo-multiplier tubes, to silicon avalanche photo-diode (Si-APD), to superconducting nanowire detectors. The efficiency of the detectors also depends on the wavelength of the light to be measured. Often detectors used to detect optical or near IR signals achieve efficiencies of ≈50 % whereas detectors for telecom wavelengths (1550 nm) can be greater than 90% for superconducting nanowires.

1.4 Conclusion

In this chapter we introduced the idea of using single photons as qubits for quantum communication. We spoke briefly of what they are and how they can be created. We then discussed QKD and how it is theoretically implemented. A select few problems with the practical implementation were addressed and we saw the channels over which this protocol can be used. The idea here was to give a very brief summary of the ideas, and the reader is welcome to investigate more into the references to gain a deeper understanding.

Chapter 2

Adaptive Optics for Quantum Key Distribution between an Earth station and a Satellite

Notes

Some material from this chapter is adapted from a project report submitted to the Canadian Space Agency [110].

This material is also forming the basis of a paper which is in preparation.

2.1 Introduction

In either the uplink or downlink scenario, with the states used for QKD encoded in photon polarization, the total number of photons collected (or equivalently, the total optical power) is the limiting factor of key generation rate. As in [89], we focus on an optical uplink to achieve satellite QKD.

Atmospheric turbulence mixes air of different temperatures and, hence, different refractive indices along the beam path, inducing phase errors in the propagating beam [98]. These phase errors have negligible impact on the beam in the near field, but their evolution creates temporal intensity fluctuations (scintillation), beam wander, and beam broadening in the far field. The impact of atmospheric turbulence on the optical power collected by an Earth station in a downlink configuration will thus be small since the phase errors are introduced primarily in the last 20 km of the beam propagation path, near Earth's surface. The impact can be significant in an uplink configuration, however, since the atmospheric wavefront error is induced primarily in the initial section the beam propagation.

Adaptive optics (AO) utilizes sensors and actuating elements to correct phase errors introduced by atmospheric turbulence. It is used extensively in astronomical observation [111], optometry [112], and has also been studied for optical communications [113]. In the latter context, AO is typically employed to minimize scintillation in order to reduce information loss. For the purpose of quantum links, short time-variable scintillation matters less than long time-averaged collected power. There are various levels of AO correction that can be applied to the optical beam, the simplest of which is correcting for beam wander as it passes through the atmosphere. This corresponds to a tip/tilt correction which is applied by fixing the lowest order terms of the Zernike polynomials (these polynomials are commonly used to model optical beam aberrations) [114]. Correction of the higher modes allows the reduction of the broadening as the beam propagates due to turbulence and will be discussed further in this chapter.

The effect of the atmosphere on the collected power of a QKD uplink to a satellite-based receiver is studied here. We consider four representative scenarios of atmospheric conditions which relate to ground station locations, and determine the impact of using an AO system to improve optical signal collection by a satellite receiver of various sizes. We begin by describing the atmospheric and orbital models followed by a discussion of the effect of the atmosphere on the beam width. Then, we look into the lower order error terms (tip/tilt) followed by the higher order errors which induce phase errors on the propagating beam. These parameters are combined and the total effect is studied and mitigation techniques are discussed.

2.2 Atmospheric and Orbital Model

The optical beam transmitted from the ground telescope passes through the atmosphere early in its optical path. The width of the beam is affected by the diffraction induced by the launch telescope aperture, and by the phase error induced by the atmospheric turbulence, which evolves into a phase and amplitude error as it propagates to the satellite in the far field.

A commonly used parameter to measure atmospheric turbulence conditions is Fried's coherence length or Fried's parameter, r_0, which depends on the refractive-index structure constant, $C_n^2(h)$ (with units of $\mathrm{m}^{-2/3}$). This structure constant represents the atmospheric turbulence strength at an altitude h which is the spectral amplitude of refractive index fluctuations within the inertial subrange of turbulence [98]. The Fried parameter also relates to the air mass that the observer is looking through, which depends on the zenith

angle of observation, ψ. For a spherical wave it is written as [105]

$$r_0 = \left[0.423k^2 \sec(\psi) \int_0^H C_n^2(h) \left(1 - \frac{h}{H}\right)^{5/3} \mathrm{d}h\right]^{-3/5}, \tag{2.1}$$

where H is the satellite altitude and k is the wavenumber. Common values of the Fried's parameter range from roughly 5 cm for a poor site to 20 cm for a very good site.

The atmospheric structure model considered is the generalized HV model [99, 115]. This model is used to generate the turbulence profiles at sea-level (HV 5-7), an average site (HV 10-10), an excellent site (HV 15-12), and Tenerife [116] (a common location for many quantum laser experiments). The numbers indicated in the HV model names (eg. HV 5-7) relate to typical values for Fried's coherence length and the isoplanatic angle in cm and µrad respectively. The HV model is calculated by the following equation:

$$C_n^2(h) = A \exp\left(-\frac{h}{H_A}\right) + B \exp\left(-\frac{h}{H_B}\right) + Ch^{10} \exp\left(-\frac{h}{H_C}\right) + D \exp\left(-\frac{(h - H_D)^2}{2d^2}\right), \tag{2.2}$$

where

- A is the coefficient for the surface or boundary layer turbulence strength, H_A is the height for its $1/e$ decay,
- B and H_B are the equivalent for the turbulence in the troposphere (up to 10 km),
- C and H_C are for the turbulence peak at the tropopause (at about 10 km),
- and D and H_D are used to define an additional isolated turbulence layer of thickness d, if required.

The parameters used for the four models are given in Table 2.1 and Figure 2.1 shows the profiles as a function of altitude. This model was designed to model experimental data and is good for a average atmospheric turbulence structure, but does not display the detail visible in atmospheric turbulence observations. It is also generally a better model for nighttime observations [117] and is less useful for daytime models.

The wind speed profile for differing heights used in our calculations is computed by adopting a Bufton wind model [115, 118, 119]. This model takes into account wind speeds at various altitudes as given by

$$v_w = v_g + v_t \times \exp\left\{-\left(\frac{h - h_{pk}}{h_{scale}}\right)^2\right\}, \tag{2.3}$$

Profile	Generalized HV model								
	A	H_A	B	H_B	C	H_C	D	H_D	d
HV 5-7	17×10^{-15}	100	27×10^{-17}	1500	3.59×10^{-53}	1000	0	-	-
HV 10-10	4.5×10^{-15}	100	9×10^{-17}	1500	2.0×10^{-53}	1000	0	-	-
HV 15-12	2.0×10^{-15}	100	7×10^{-17}	1500	1.54×10^{-53}	1000	0	-	-
Tenerife	9.42×10^{-15}	100	27×10^{-17}	1500	2.50×10^{-53}	1000	0	-	-

Table 2.1: Turbulence parameters used for the HV models [115]. Tenerife is a common location for many quantum laser experiments [116].

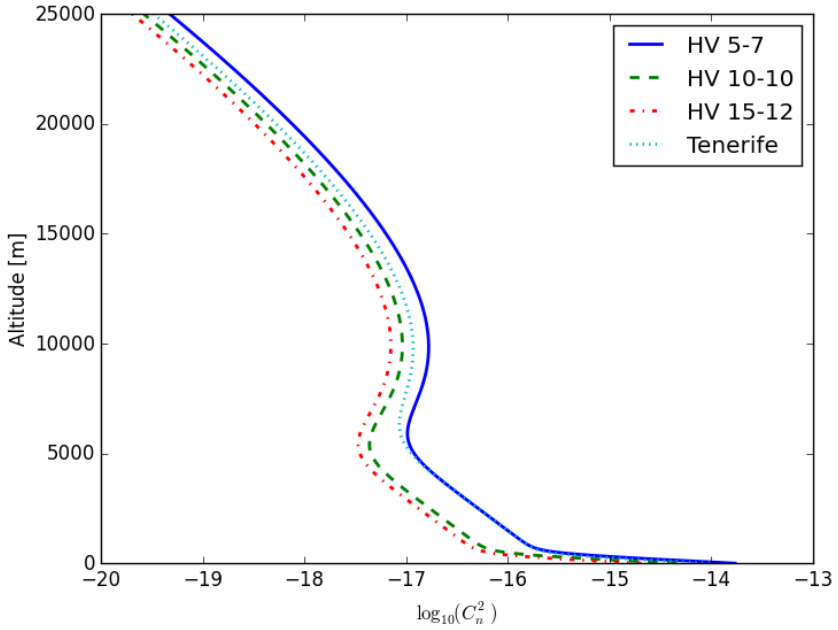


Figure 2.1: Hufnagel Valley structure function, $C_n^2(h)$, profiles for a sea level site (HV 5-7), an average site (HV 10-10), an excellent site (HV 15-12), and a location on Tenerife.

Parameter name	Symbol	Default Value
Ground speed wind	v_g	5 m/s
Altitude of the peak	h_{pk}	9400 m
Scale height	h_{scale}	4800 m

Table 2.2: Parameters for the Bufton wind speed model and their default values.

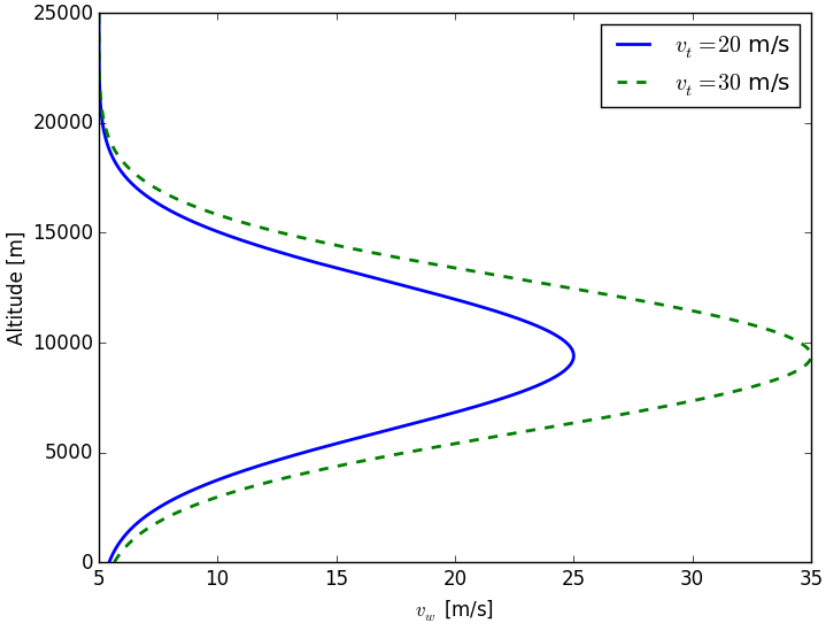


Figure 2.2: Bufton wind functions, v_w, for profiles with tropopause wind speeds of 20 m/s and 30 m/s.

where h is the altitude and v_t is the tropopause, or high altitude, wind speed and the remaining parameters and their default values can be found in Table 2.2. Figure 2.2 shows the wind speed profiles for tropopause wind speeds, v_t, of 20 m/s and 30 m/s.

We use a simplified model of a satellite orbiting a spherical Earth. The mass of the Earth is given as 5.97×10^{24} kg and the mean radius as 6.37×10^6 m. A satellite orbiting a spherical planet will have angular velocity given by

$$\omega = \sqrt{\frac{Gm_e}{l_o^3}} \tag{2.4}$$

where m_e is the mass of the Earth and l_o is the orbital radius from the center of the planet. The position and distance of the satellite can be calculated simply by knowing its angle from zenith at the ground station location, and the orbital height from the surface of the

planet.

For the anisoplanatic error described further on, it will be important to calculate the angle the satellite has moved by the time the beacon signal propagates to the ground station, the system measures the correction for AO and applies the correction to the uplink signal, and the signal reaches the satellite. This angle is determined based on the time it takes light to propagate from the satellite to the ground station, and back up to the satellite. This time is then used along with the angular velocity of the satellite to calculate the angle propagated, relative to the ground station, by the satellite.

2.2.1 Atmospheric Effect on Beam Width

For an initially Gaussian beam, the long-term $1/e^2$ Gaussian beam width (spot radius), w_{LT}, when it reaches the satellite at a distance, L, is computed by convolving the diffraction-limited width, $w_{\mathrm{diff}}(z) = w_0\sqrt{1+(z/z_0)^2}$, with the phase-error beam widening from the atmospheric turbulence. This yields [120, 121]

$$w_{\mathrm{LT}}(z=L) = \sqrt{w_0^2\left(1+\frac{L^2}{z_0^2}\right)+2\left(\frac{4L}{kr_0}\right)^2}, \tag{2.5}$$

where w_0 is the beam waist, z_0 is the Rayleigh distance, and k is the wavenumber. Note that we neglect the defect from the launch telescope aperture cutting off the edge of the Gaussian beam as the effect is small compared to the other contributions considered.

The efficiency of the link is defined as the ratio of the received power, P_r, over the transmitted power, P_t, in dB, and is computed from the beam width at the satellite

$$\epsilon = 10\log_{10}\left(\frac{P_r}{P_t}\right), \tag{2.6}$$

$$= 10\log_{10}\left(\eta_r\eta_t\eta_0^{\sec\psi}\frac{D_r^2}{w_{\mathrm{LT}}^2}I\right), \tag{2.7}$$

where I is a correction factor to account for residual jitter described below, η_r is the receiver optical transmittance, η_t is the transmitter optical transmittance, η_0 is the optical transmittance at zenith, and D_r is the receiver aperture diameter . The atmospheric contribution to beam widening and link efficiency is a function of r_0, which is highly dependent on the altitude and topography of the site where the transmitter telescope is located. Figure 2.3 shows the long-term beam waist, w_{LT}, the divergence of the beam as well as the link efficiency from Equation 2.6 as a function of elevation angle. From this it

Parameter	symbol	value
Satellite altitude (km)	H	600
Receiver aperture diameter (m)	D_r	0.4
Receiver optical transmittance	η_r	0.5
QKD signal wavelength (µm)	λ	0.785
Transmitter aperture diameter	D_t	0.25
Transmitter optical transmittance	η_t	0.5
Optical transmittance at zenith	η_0	0.8
Average wind speed (m/s)	v_t	20
Turbulence Model	$C_n^2(h)$	HV 5-7

Table 2.3: Summary of the ground-to-satellite link baseline parameters for the simulations. These parameters are used in the simulation unless otherwise stated and are derived from previous studies [88, 89].

can easily be seen that turbulence has a strong effect on the beam. For example, a beam starting from a transmitter of 25 cm and reaching a satellite at 600 km at a 45° angle from zenith would be nearly 10 m.

The average value of I, computed by assuming that the 1D residual jitter has Gaussian statistics that are added in quadrature to the beam width [122], can be calculated as

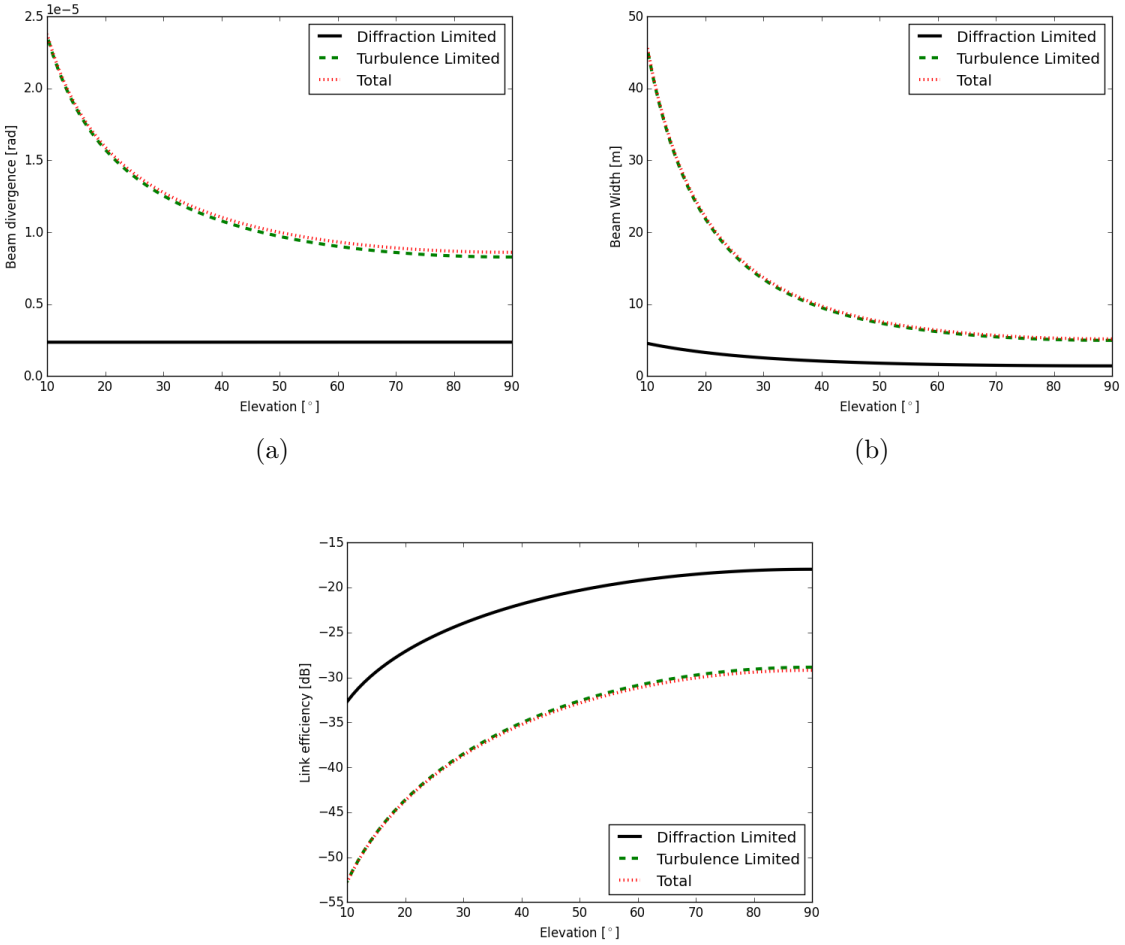
$$\langle I \rangle = \frac{\beta}{\beta + 1}, \tag{2.8}$$

where

$$\beta = \frac{1}{8}\left(\frac{\Theta}{\sigma_j}\right)^2, \tag{2.9}$$

and Θ is the beam divergence and σ_j is the 1D residual jitter standard deviation.

Unless otherwise stated, the parameters we will be using for our simulations are given in Table 2.3.



(a) (b)

(c)

Figure 2.3: Impact of turbulence on the beam (a) divergence, (b) width and (c) link efficiency. This simulation uses the long-term beam width including diffraction and beam broadening by turbulence. The black curve signifies the diffraction limit while the green curve signifies the turbulence limit. The total effect is seen in the red curve. The simulation uses an HV 5-7 model for a satellite at 600 km. Note: I is set to one in these plots.

2.3 Beam Wander Correction

The simplest correction that can be implemented to the propagating beam is tilt, or beam wander, compensation. The fine tracking system corrects the direction of the ground transmitter in a closed-loop by using the down-link beacon from the satellite as a reference. The atmospheric tilt within the bandwidth of this system will be compensated in this process.

In order to treat the beam wander, we must separate the tilt (wander) contribution from the beam spread, which is induced by higher order phase aberrations (higher order in Zernike modes, to be described in Section 2.4) and discussed in the next section. In this fashion, the long-term beam width can be seen as a short term-beam width that is broadened by the beam wander. This short-term beam width can be given by [121, 123]

$$w_{\mathrm{ST}}(z=L) = \sqrt{w_0^2\left(1+\frac{L^2}{Z_0^2}\right)+2\left(\frac{4.2L}{kr_0}\left[1-0.26\left(\frac{r_0}{w_0}\right)^{1/3}\right]\right)^2}. \tag{2.10}$$

where the first term is the diffraction spread, the first half of the second term is the beam spreading, and the second half of the second term is the beam wander. This assumption is valid when $0.26(r_0/w_0)^{1/3} << 1$.

By replacing the long-term beam spread in Equation 2.6 with the short-term value and assuming perfect pointing, there is only a 1 dB improvement if the tilt were to be perfectly corrected. This leads to the conclusion that if only the tilt error is compensated, the improvement will be minor, however, it is still beneficial to construct a detailed model of this correction to simulate the best possible performance.

The extent to which the beam wander can be corrected depends primarily on four error sources: the limited signal-to-noise ratio of the sensor measurement (σ_{SNR}), the correction system limited bandwidth ($\sigma_{\mathrm{tilt\ delay}}$), centroid anisoplanatism (σ_{CA}), and anisoplanatism ($\sigma_{\mathrm{tilt\ ani}}$).

The first of these errors, σ_{SNR}, is contingent on the choice of commercially available position sensitive detectors (PSD). These devices can typically achieve $\sigma_{\mathrm{SNR}} < 0.15\,\mu\mathrm{rad}$ with bright sources and this value will be assumed in our model.

The correction system limited temporal bandwidth, $\sigma_{\mathrm{tilt\ delay}}$, is caused by the atmospheric tilt evolving from the time it is read by the sensor to the moment the correction is applied. For a closed loop correction with a bandwidth f_{c}, this is calculated as [124]

$$\sigma_{\mathrm{tilt\ delay}} = \frac{f_{\mathrm{T}}}{f_{\mathrm{c}}}\frac{\lambda}{D_t}, \tag{2.11}$$

Bandwidth	20 Hz	40 Hz	60 Hz	80 Hz	100 Hz
$\sigma_{\text{tilt delay}}$[µrad]	0.93	0.47	0.31	0.23	0.19

Table 2.4: Tilt error due to closed loop delay for different system bandwidths. The satellite is at zenith.

where f_{T} is the tracking frequency, defined as the frequency at which the tilt standard deviation is equal to the diffraction limited point-spread-function (PSF) full-width-at-half-maximum (FWHM), λ is the wavelength, and D_t is the ground transmitter telescope diameter. For given wind speed $v_w(h)$ and $C_n^2(h)$ profiles, the tracking frequency is

$$f_{\text{T}} = 0.331 D_t^{-1/6} \lambda^{-1} \left[\sec\psi \int_0^H C_n^2(h) v_w^2(h) \mathrm{d}h \right]^{1/2}. \tag{2.12}$$

Expected 1D values for $\sigma_{\text{tilt delay}}$ for an observation at zenith with different loop bandwidths are given in Table 2.4.

The higher order wavefront errors induced by turbulence eddies smaller than the aperture of the emitter telescope changes the PSF shape incident on the PSD that leads to centroid estimate errors, or *centroid anisoplanatism errors*, σ_{CA}. The one-dimensional standard deviation of this error term is given by [125, 126]

$$\sigma_{\text{CA}} = 5.51 \times 10^{-2} \left(\frac{\lambda}{D_t} \right) \left(\frac{D_t}{r_0} \right)^{5/6}. \tag{2.13}$$

This term is mostly dependent on the turbulence strength as determined by the Fried parameter, and is ∼0.4 µrad for an HV 5-7 model when the satellite is at Zenith.

The motion of the satellite means that the down-link beacon from the satellite will take a different path than the up-link beacon from the ground station. This leads to *anisoplanatic* error, $\sigma_{\text{tilt ani}}$. This error is computed by the procedure described in [125] and is given as

$$\sigma_{\text{tilt ani}} = 6.14 D_t^{-1/6} \left[\sec\psi \int_0^H C_n^2(z) f_\Delta(z) \mathrm{d}z \right]^{1/2}, \tag{2.14}$$

where f_Δ is a weighting function given for a circular aperture (such as our telescope) and is

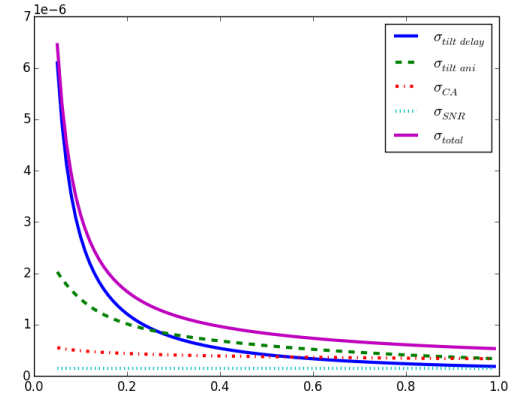
$$\begin{aligned} f_\Delta(z) &= \int_0^{2\pi} \int_0^1 \{ \frac{1}{2} [u^2 + 2us\cos w + s^2]^{5/6} \\ &+ \frac{1}{2} [u^2 - 2us\cos w + s^2]^{5/6} - u^{5/3} - s^{5/3} \} \\ &\times u[\cos^{-1} u - (3u - 2u^3)\sqrt{1-u^2}] \mathrm{d}u\mathrm{d}w, \end{aligned} \tag{2.15}$$

where

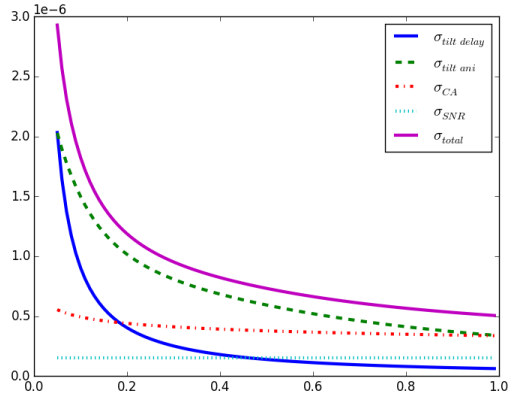
$$s = \frac{z\theta \sec \psi}{D_t}. \tag{2.16}$$

Assuming $\theta = 50\,\mu\text{rad}$ between the two beams at zenith, $\sigma_{\text{tilt ani}}$ is approximately 1 µrad. Some measurements reported in the literature [127] demonstrate this value could be as much as three times higher than the one given by this model. This error source can be reduced by selecting a site with weaker turbulence or by using a larger aperture on the ground.

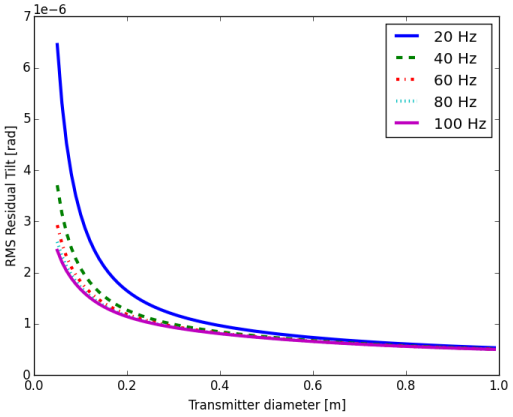
Figure 2.4 shows the contributions of these errors to the total root mean square (RMS) tilt error for different correction bandwidths. The total link efficiency as per Equation 2.6 is also plotted for different correction bandwidths. One can see that the bandwidth effects which term is the dominant error in the system. At low transmitter diameters (between 10 cm and 20 cm) $\sigma_{\text{tilt delay}}$ is the dominant error for a bandwidth of 20 Hz, but when the bandwidth is increased to 60 Hz the $\sigma_{\text{tilt ani}}$ term dominates. As the diameter increases, the dominant error term changes. It can also be seen that increasing the bandwidth above 60 Hz does not increase the link efficiency significantly and therefore further increases are unnecessary.



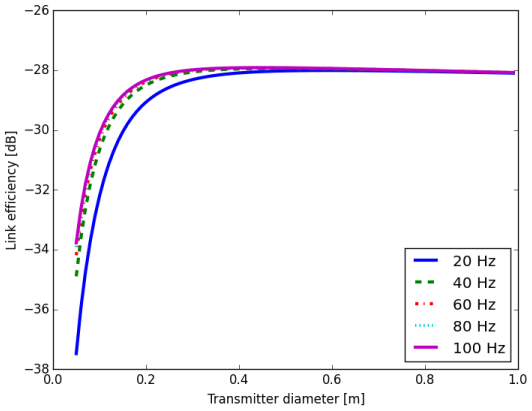
(a) Bandwidth = 20 Hz



(b) Bandwidth = 60 Hz



(c)



(d)

Figure 2.4: Contributions for the different tilt error sources to the total residual tilt error is shown in the top two panels for (a) 20 Hz correction bandwidth and (b) 60 Hz correction bandwidth. (c) Shows the RMS residual tilt from all the sources for various correction bandwidths and (d) the link efficiency for various correction bandwidths. The results are shown for different ground transmitter diameters. The satellite orbiting at 600 km and is located momentarily at zenith.

2.4 Higher Order Phase Corrections

We attempt to correct for higher order wavefront aberrations in our model with the use of an AO system. The PSF delivered by such a system is modeled by a diffraction limited core surrounded by a seeing-limited halo [98]. The Strehl ratio is defined as the fraction of intensity that is in the diffraction-limited core compared to the perfectly corrected system. For a given RMS wavefront error with σ in radians (where 2π radians equates to an error of λ), the Strehl ratio is evaluated from the Mahajan equation [128]

$$S \approx e^{-\sigma^2}. \tag{2.17}$$

A better correction of the wavefront by the AO system reduces σ, increases the Strehl ratio, and hence increases the fraction of power that is within the launch telescope diffraction-limited core. The approximation does not include the Strehl reduction due to tip/tilt errors as discussed in the previous section, therefore the factor I (Equation 2.8) is conserved and described as before.

We consider three primary sources of error when developing a model to compute the Strehl ratio of an AO system: the time delay error ($\sigma_{\text{AO delay}}$), the spatial fitting error (σ_{fit}), and the anisoplanatic phase error ($\sigma_{\text{phase ani}}$).

The time delay error is similar to the tilt error in the previous section. It is caused by the atmospheric turbulence evolution between the time the wavefront error is read and the time it is corrected. In the case of higher-order aberrations, the tracking frequency is replaced by the Greenwood frequency (the optimal correction bandwidth for AO) [98, 129],

$$f_{\text{G}} = 2.31\lambda^{-6/5}\left[\sec\psi \int_0^H C_n^2(h) v_w^{5/3}(h) dh\right]^{3/5}. \tag{2.18}$$

The associated wavefront error term is [98, 130]

$$\sigma_{\text{AO delay}} = \left(\frac{f_{\text{G}}}{f_{\text{c}}}\right)^{5/6}. \tag{2.19}$$

This is mainly dependent on the wavelength and the turbulence strength. Table 2.5 shows values for $\sigma_{\text{AO delay}}$ at different bandwidths.

The spatial fitting error is caused by the limited degrees of freedom of the wavefront corrector. Assuming a modal control based on the Zernike modes [98, 114] and a system that can perfectly correct the modes that it reproduces, the residual wavefront error after correction of a number of modes under Kolmogorov turbulence is given by [131]

$$\sigma_{\text{fit}} = \left[0.2944 J^{-\sqrt{3}/2}\left(\frac{D_t}{r_0}\right)^{5/3}\right]^{\frac{1}{2}} \text{(rad)} \tag{2.20}$$

Bandwidth	20 Hz	40 Hz	60 Hz	80 Hz	100 Hz
λ=0.785 µm	1.61 rad	0.91 rad	0.65 rad	0.51 rad	0.42 rad
λ=1.5 µm	0.84 rad	0.47 rad	0.34 rad	0.27 rad	0.22 rad

Table 2.5: Closed loop delay wavefront error in radians for different correction bandwidths. The satellite orbiting at 600 km and is located momentarily at zenith.

where J is the number of Zernike modes corrected (for $J > 10$). A table of values for σ_{fit} up to $J = 21$ can be found in [131]. Figure 2.5 shows the Strehl value from the σ_{fit} for different numbers of Zernike modes corrected as well as the resulting link efficiency from correcting only these errors. Figure 2.5 shows the effect of correcting an increasing number of Zernike modes for various transmitter telescope diameters. Increasing the number of modes one wants to correct requires an increase in the number of actuators in the deformable mirror used to implement the correction, this factor can be limited by available technology and cost. Increasing beyond correcting 45 modes there is no significant increase in the link efficiency performance for the diameters shown ($<$ 2 dB for larger diameters) and can therefore be chosen as the default number of modes to correct.

Two wavelengths are shown in Figure 2.5 relating to our chosen 785 nm and the common telecommunications wavelength at 1500 nm. The Strehl ratio's at 1500 nm show more of the light is in the diffraction limited core, but the core is larger at this wavelength which increases the overall loss.

The anisoplanatic phase error again arises from differences between the propagation path of the reference beam with respect to the corrected beam. By correcting the phase for a different portion of atmosphere, the error can in fact be greater than no correction at all. The anisoplanatic phase error is computed as

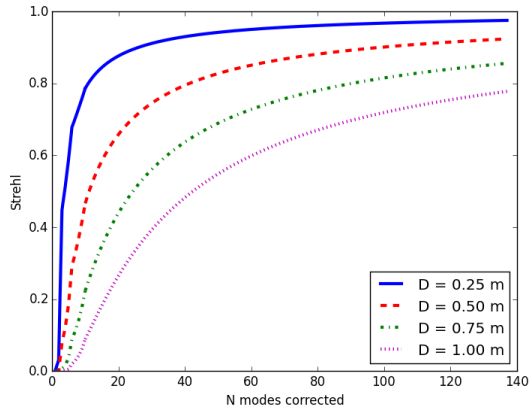
$$\sigma_{\text{phase ani}} = \left(\frac{\theta}{\theta_0}\right)^{5/6}, \tag{2.21}$$

where θ is the angular path difference between the reference beam and the corrected beam and

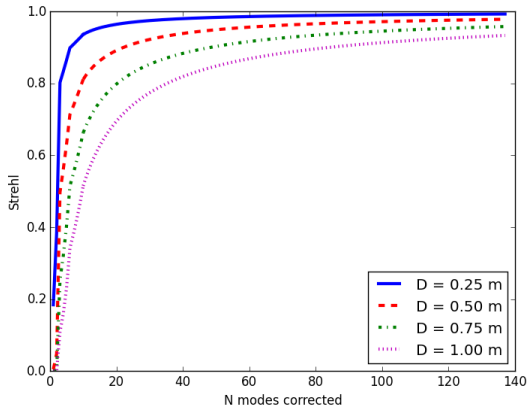
$$\theta_0 = \left[2.91k^2(\sec\psi)^{8/3}\int_0^H C_n^2(z)z^{5/3}\mathrm{d}z\right]^{-3/5}. \tag{2.22}$$

The isoplanatic angle, θ_0, is the angle where the wavefront variance between the reference beam and object is 1 rad^2.

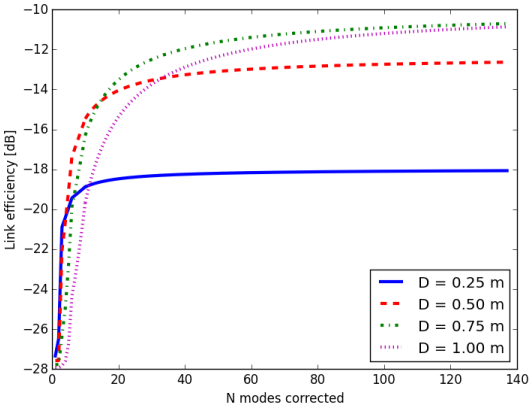
Now that these phase errors have been described, we need a link efficiency equation to determine the benefits of AO. We modify Equation 2.6 to take into account the diffraction



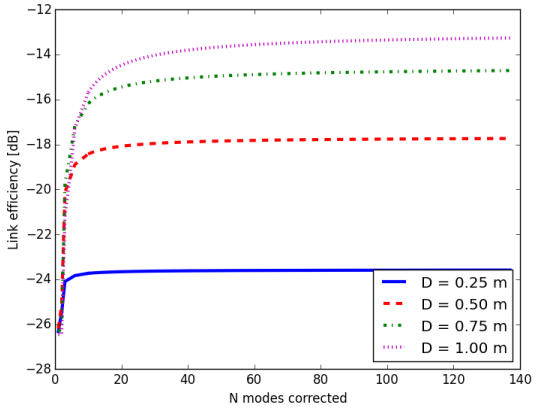
(a) Wavelength = 785 nm



(b) Wavelength = 1500 nm



(c) Wavelength = 785 nm



(d) Wavelength = 1500 nm

Figure 2.5: The Strehl ratio obtained from the spatial fitting error for different number of Zernike modes corrected and for different launch telescope diameters is shown in the top two panels. The resulting link efficiency is plotted in the bottom panel for (c) 785 nm and (d) 1500 nm. The satellite is at zenith.

limited central peak and the seeing limited halo to get a link efficiency of

$$\epsilon = 10\log_{10}\left(\frac{P_r}{P_t}\right), \tag{2.23}$$

$$= 10\log_{10}\left(\eta_r\eta_t\eta_0^{\sec\psi}D_r^2\left[\frac{1}{w_{\text{diff}}^2}I_{\text{diff}}S + \frac{1}{w_{\text{ST}}^2}I_{\text{ST}}(1-S)\right]\right), \tag{2.24}$$

where w_{diff} is the diffraction-limited PSF width and w_{ST} is given in Equation 2.10. I_{diff} and I_{ST} are used to compute the energy loss due to jitter for the diffraction-limited core and the short-term seeing limited halo, respectively. As the AO correction becomes less effective (S decreases), more of the power spreads into the halo.

2.5 Adaptive Optics Analysis

In this section, the model described in the previous sections is used to evaluate the impact of different parameters on the link efficiency. It is assumed throughout this analysis that the AO system is correcting the first 45 Zernike modes, the system correction bandwidth is 60 Hz, and the satellite orbits at an altitude of 600 km. We also use a transmitter diameter of 50 cm for this section as opposed to 25 cm in the previous sections. This increase in diameter showed the optimal link efficiency for the tilt errors and showed significant improvement from the 25 cm diameter telescope for the higher order phase errors. Before studying adaptive optics, increasing the transmitter from 25 cm to 50 cm showed no improvement due to the atmospheric turbulence but an improvement can be seen here as will be discussed further on.

The link efficiency variation with satellite elevation is computed from 10° to 90° elevations and the results are shown using the same common legend for all the explored scenarios. The expected link efficiency for a diffraction limited beam (perfect wavefront correction in both tilt and phase) is plotted in solid black and shows the maximal performance that can be achieved. This is represented in Equation 2.24 by setting I_{diff}, I_{ST}, and S to 1. A full correction for phase and tilt with the limiting errors as described in the previous sections is plotted in solid cyan, implying that I_{diff}, I_{ST}, and S are all less than 1. The dashed red lines signify if the phase errors are not corrected ($S = 0$) but the tilt errors are corrected as described ($I_{\text{diff}} < 1$ and $I_{\text{ST}} < 1$). The dash-dot magenta line signifies perfectly correcting the phase errors ($S = 1$) and correcting the provided system limited tilt errors ($I_{\text{diff}} < 1$ and $I_{\text{ST}} < 1$). Lastly, the dotted green lines represent the efficiency if the anisoplanatism error is perfectly corrected, but all other errors remain the same.

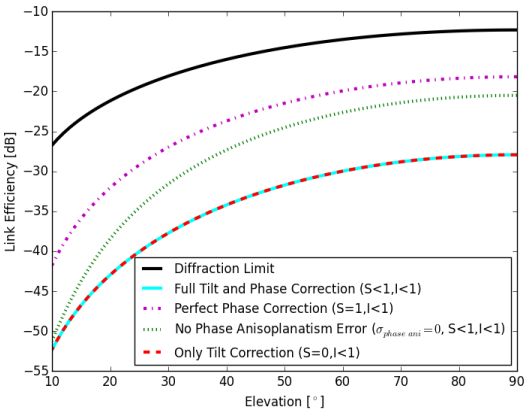
Figure 2.6 shows the link efficiencies as corrected for different turbulence strengths. A first result from this analysis is that the turbulence strength and, hence, the site selection can have a significant impact on the link efficiency improvement. A gain of approximately 10 dB is found for a good astronomical site (HV 15-12) compared to a site at sea-level (HV 5-7 model).

A second result is that the AO performance is strongly limited by anisoplanatism. In fact, there is no gain in using an AO system if this term is not mitigated. Even worse, this strong contribution of the anisoplanatism error is symptomatic of a weak correlation between the turbulence in the down-link and up-link paths. In such a case, the AO system can even worsen the wavefront in the up-link beam which would result in a link efficiency loss. This holds as well for the tilt error, which is also dominated by anisoplanatism [132]. The current model does not allow us to simulate such performance degradation but this could be simulated with Monte Carlo methods by propagating both beams through atmospheric phase screens conjugated to a few discrete altitudes, for example. A third result is that an improvement of 5 dB to 8 dB is expected from an AO system if the phase anisoplanatic error can be perfectly corrected.

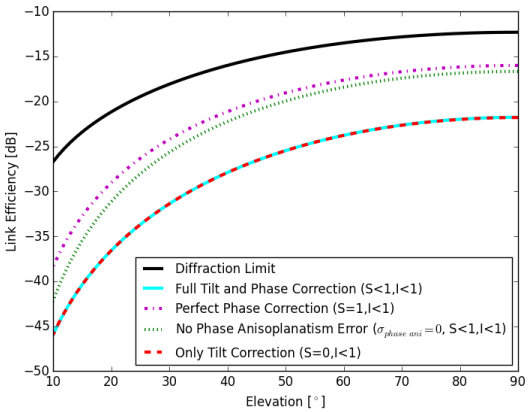
The analysis was then extended to a lower orbit and to other transmitter sizes on the ground. The results of a lower orbit of 400 km (similar to the International Space Station) in Figure 2.7 show little difference, approximately 3 dB, compared to the 600 km orbit.

A bigger transmitter size (seen in Figure 2.8) has the potential to allow better AO correction. The improvement is of about 1 dB if the diameter is increased from 0.50 m to 0.75 m, and another 1 dB improvement is obtained if it is increased to 1 m. The most important improvement comes from increasing the diameter from 0.25 m to 0.50 m for which a 4 dB improvement is found (when neglecting anisoplanatism error).

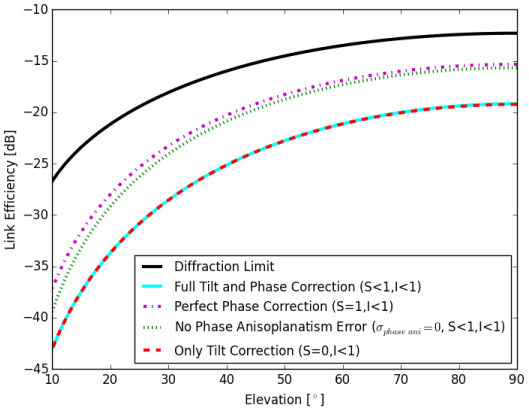
As mentioned above, it is critical to reduce the anisoplanatic error term for an AO system to be useful. A typical and mature approach to reduce this error term in astronomical applications is to use a reference laser guide star (LGS) to sample the turbulence in the proper atmospheric path. This LGS can be generated by exciting a 90 km altitude sodium layer with a laser or to use a time gating camera to observe the Rayleigh backscatter of a pulsed laser at a typical altitude of 18 km. While this LGS mitigates the anisoplanatic error, a new error term needs to be considered due to the difference in altitude between the satellite and the LGS. This results in a different path taken through the atmosphere by the light emitted by the LGS and captured by the telescope and the quantum beam traveling to the satellite. This error term is referred to as focal anisoplanatism, or cone



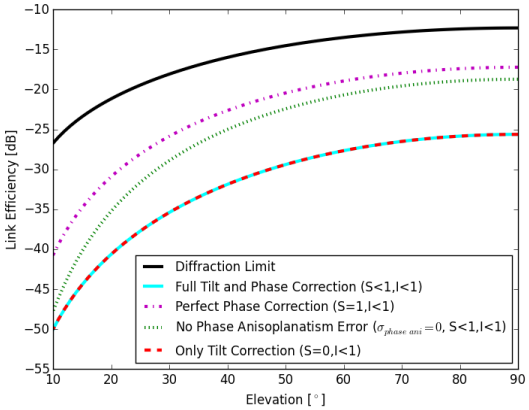
(a) HV 5-7



(b) HV 10-10

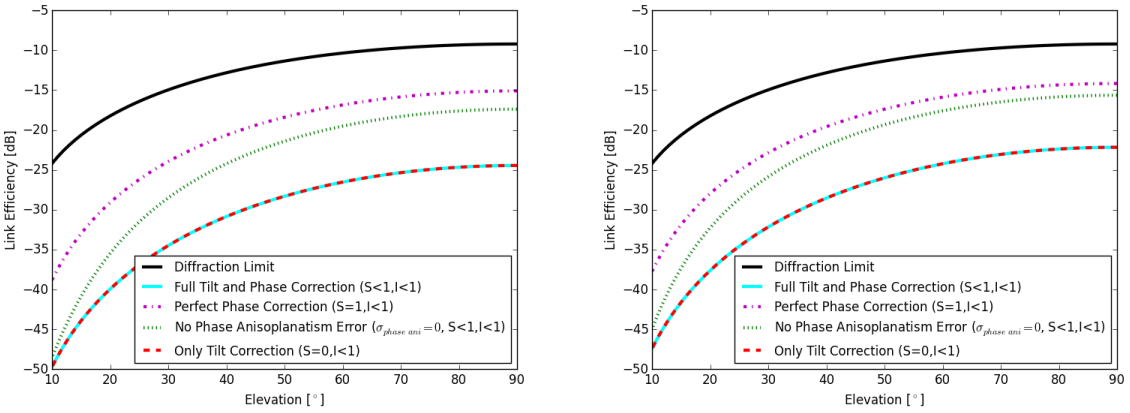


(c) HV 15-12



(d) Tenerife

Figure 2.6: Prediction of the loss as a function of elevation angle with AO. (a) HV 5-7 models a typical sea-level site, (b) HV 10-10 is a typical good site, (c) HV 15-12 is an excellent site, and (d) Tenerife is the measured median turbulence strength at the island of Tenerife in the Canary Islands.



(a) HV 5-7 (b) Tenerife

Figure 2.7: Prediction of the loss as a function of elevation angle with AO at 400 km, for different HV models.

effect and is given as [98]

$$\sigma_{\text{cone}} = \left(\frac{D_t}{d_0}\right)^{5/6}, \tag{2.25}$$

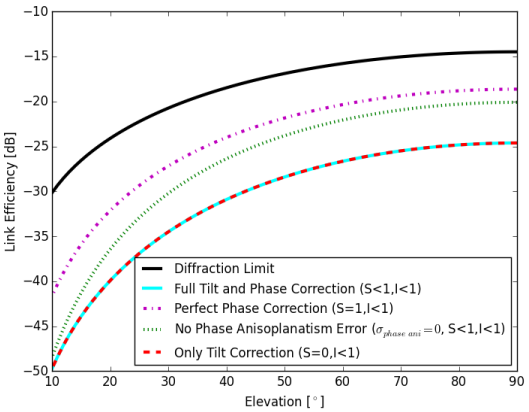
where

$$d_0 = \lambda^{6/5} \cos^{3/5} \psi \left(19.77 \int_0^H C_n^2(h) \left(\frac{h}{\text{LGS}_{\text{height}}}\right)^{5/3} \mathrm{d}h\right)^{-3/5}. \tag{2.26}$$

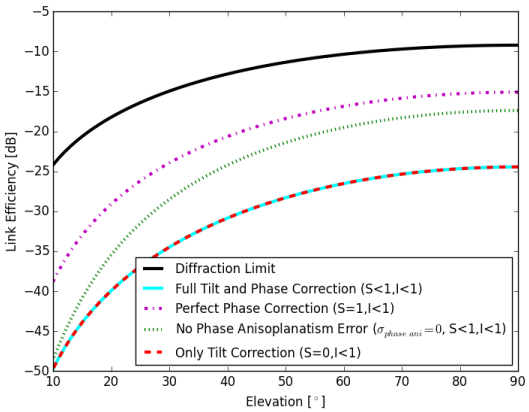
The generated LGS also cannot be used as a reference for tilt correction since the exact LGS location is unknown due to the laser beam being affected by some tilt in both its upward propagation (on its way to generate the LGS) and its downward propagation. The wavelength chosen for this down-link beacon can have a small impact on the tilt anisoplanatic error due to the differential atmospheric dispersion of the atmosphere when the satellite is at low elevations. However, this contribution is expected to be small.

Figure 2.9 and Figure 2.10 show the AO performance when using a Rayleigh LGS at an altitude of 18 km and 30 km respectively (solid cyan line). They show a significant improvement over the previous results without the LGS.

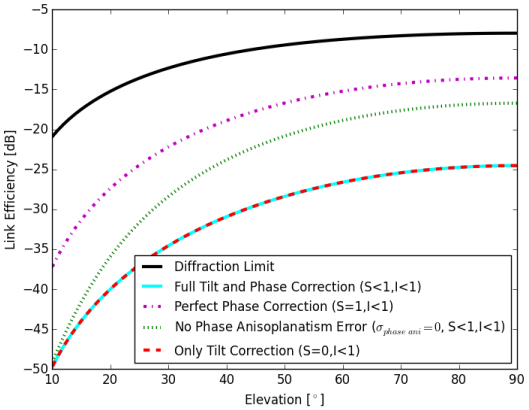
Another interesting point to investigate would be the use of geostationary satellites. A geostationary satellite orbits the Earth at approximately 35 000 km and has the same orbital period as the Earth's rotational period. As a consequence, it appears stationary in the sky relative to a ground station. If the satellite is not moving relative to the ground station, this eliminates the problem of passing through different portions of the atmosphere (the timing of the pass is still taken into account through the delay error terms). Figure



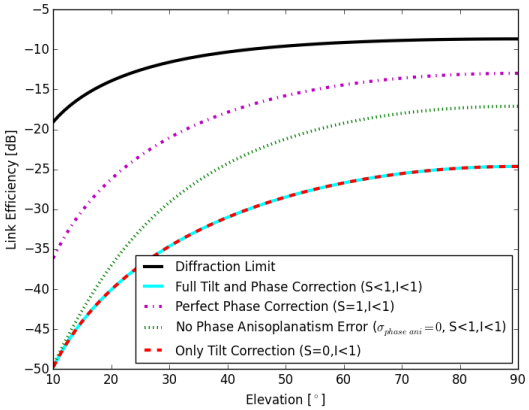
(a) D = 0.25 m



(b) D = 0.50 m

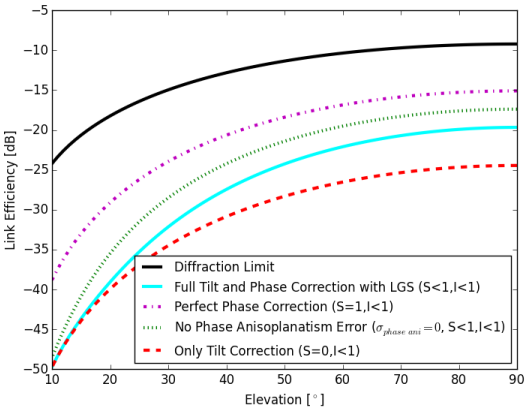


(c) D = 0.75 m

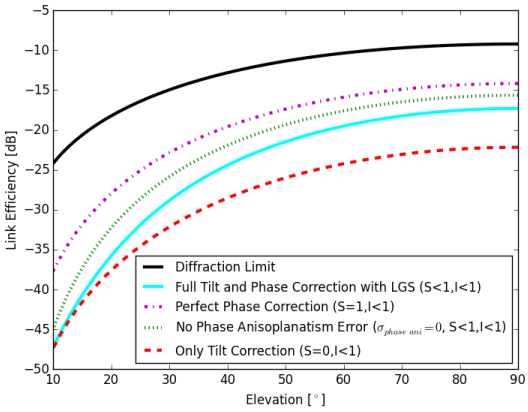


(d) D = 1.00 m

Figure 2.8: Prediction of the loss as a function of elevation angle with different transmitter diameters. (a) 25 cm, (b) 50 cm, (c) 75 cm, and (d) 100 cm. The largest improvement can be seen between the 25 cm and 50 cm diameter transmitters. The satellite orbiting at 600 km and is located momentarily at zenith.

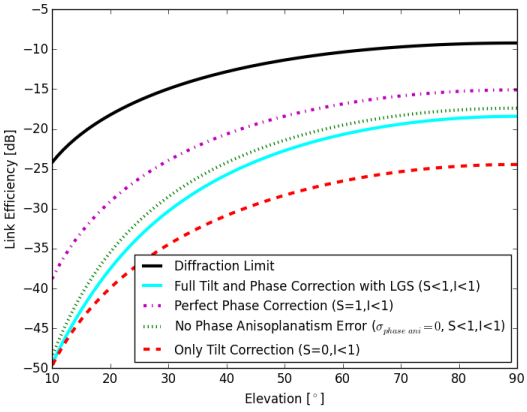


(a) HV 5-7

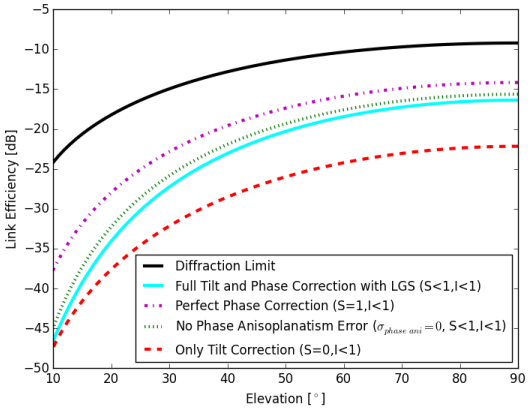


(b) Tenerife

Figure 2.9: Prediction of the loss as a function of elevation angle with AO using a Rayleigh LGS at 18 km altitude. The performance difference between the cyan line (that corresponds to a system without anisoplanatic error) and the green curve (that corresponds to the performance of an AO system with a Rayleigh LGS) is due to the cone effect.

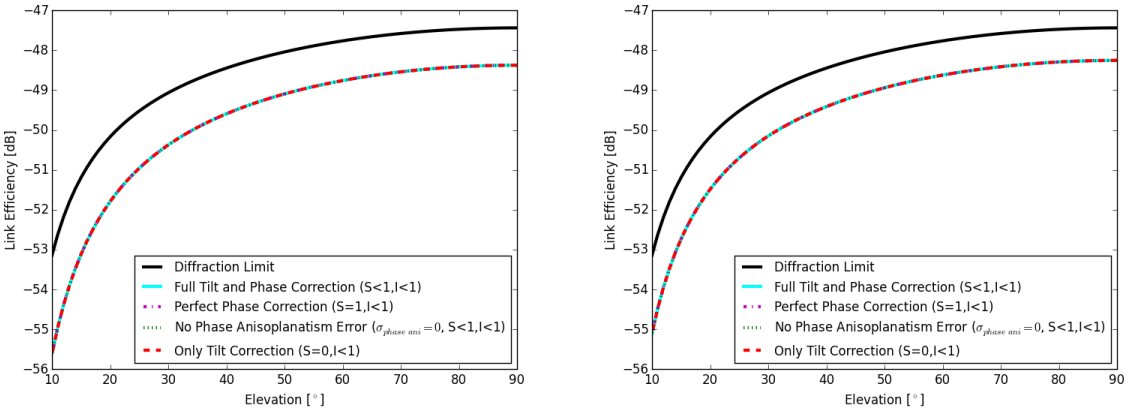


(a) HV 5-7



(b) Tenerife

Figure 2.10: Prediction of the loss as a function of elevation angle with AO using a Rayleigh LGS at 30 km altitude. The performance difference between the cyan line (that corresponds to a system without anisoplanatic error) and the green curve (that corresponds to the performance of an AO system with a Rayleigh LGS) is due to the cone effect.



(a) HV 5-7

(b) Tenerife

Figure 2.11: Prediction of the loss as a function of elevation angle with AO using a geostationary satellite. This eliminates the problem of anisoplanatism as the satellite does not move relative to the ground station.

2.11 demonstrates the use of a geostationary satellite and shows that the anisoplanatism no longer dominates the error in correction.

While the loss overall is larger due to the longer distance to the satellite, the system is now limited by the other error terms, especially the bandwidth of the system, many of which are technological and can be improved with time and proper equipment.

2.6 Discussion

The analytical model used here is useful to quickly explore a wide range of parameters and narrow down the ones that are the most likely to yield the best results for an optical up-link for QKD to a satellite. It was noticed that after a point increasing the diameter of the telescope no longer yields a useful increase in performance. This is limited by the Fried's coherence length and for many sites studied here shows the best improvement to be around 0.5 m with adaptive optics (this can vary depending on other parameters like the distance of the LGS, but 0.5 m is a decent starting point).

A major effect is the level of atmospheric turbulence, and by choosing a site with weaker turbulence, one can improve the link efficiency quite drastically. In the four sites studied, the HV 15-12 site performed the best, but is equivalent to an extremely good high altitude site and may be difficult to access.

The dominant effect inhibiting the usefulness of AO is the anisoplanatism error. If this error cannot be corrected, there is no real gain to using an AO system. Two ways to mitigate this effect are to use a LGS which is generated in the path which the optical up-link will pass through, and the other is using a geostationary satellite. The former option is quite well established in astronomy and has multiple options. This study looked into the Rayleigh guide star which can be implemented fairly easily. The geostationary option provides far more geometrical loss which might be too much to tolerate. Also, it is not always feasible to obtain geostationary satellites as they are very expensive, and space in that orbital plane is very limited.

The satellite orbital model presented here is a very simplified model which assumes no rotation of the Earth during the satellite pass, as well as a perfectly spherical Earth. In order to properly model the pass, real data of satellite orbits can be used and input into the analysis showing a more realistic flight path.

2.7 Conclusion

We have studied the impact of atmospheric turbulence on the link efficiency and the capability of an AO system to compensate its effects from an analytical perspective. This allowed evaluating that a 10 dB link efficiency improvement is possible changing a site at sea-level for an excellent astronomical site. In the case where the site is predetermined or that further improvement is desired, an AO system can be used to increase the efficiency by a factor of up to 5 dB. It is mandatory, however, to correct for anisoplanatism for the AO system to be useful. One possible approach to achieve this is to use a Rayleigh LGS as a reference in front of the satellite to estimate the turbulence in the quantum beam path, but this cannot give information on the tilt anisoplanatism. This approach has been demonstrated in astronomical applications. Although financially and technically challenging, another option is to use a geostationary satellite if one is able to tolerate the larger geometrical loss due to the farther distance.

Chapter 3

A Fine Pointing System Suitable for Quantum Communications on a Satellite

Notes

Some material from this chapter was published in the PhD thesis of Sarah Kaiser [133] and a project report submitted to the Canadian Space Agency [134].

This material is also forming the basis of a paper which is in preparation.

3.1 Introduction

The objective of the Quantum Encryption and Science Satellite (QEYSSAT) mission [88] is to create a quantum link between a Low Earth Orbit (LEO) satellite and a ground station using optical polarization at the single photon level. The quality of this link depends on, among other parameters, the accuracy of pointing the source and receiver towards each other. The quantum link budget developed in previous studies [89] recommends pointing accuracies of 2 µrad at the ground-based transmitter and 20 µrad at the receiver on the satellite.

Achieving these accuracies requires closed-loop target tracking with a range of motion at least equal to the open-loop coarse tracking error of the satellite, which could be a telescope gimbal or the slew of the satellite bus, and a bandwidth high enough to compensate for residual jitter. Closed-loop pointing will be achieved by tracking a beacon signal located at, and typically aligned with, the quantum source or receiver at the opposite end of the link. The beacon and quantum signals will both pass through corrective optics that are

adjusted to maintain the optical alignment by a control loop fed from the readout of a beacon position detector.

Not only should this fine pointing unit (FPU) ensure the fidelity of the QKD protocol it is intended to support, it should be designed to be "flight-like" in form, fit, and function and must interface with the QKD receiver integrated optical assembly (IOA) prototype developed in a previous study.

3.2 Requirements

Fine pointing systems are required in many laser communications applications to satellites. These devices guide the light to the various detector technologies and prevent as much loss as possible once the light is collected. Generally, classical-laser FPU's do not require high-fidelity preservation of the polarization of light, but they are more concerned with drop-outs than the QKD protocol that we consider. A survey of devices was conducted to examine the current state of laser communication FPU's to determine if a similar system could be created for a quantum link.

The devices from this study used a variety of techniques to guide the beam, such as a mirror moved by voice coils [135], piezoelectric actuators [136], permanent magnets with coils [137], electromagnetic actuators [138, 139], inertial sensors [140, 141], orbital information [142], and gimbal mounts (coarse pointing) [143]. An implementation to an airborne platform has also been demonstrated with a fast steering mirror (FSM) [144,145].

The devices listed above have a range of accuracies, sizes, and functionalities. Some offer fields of view on the order of a few degrees down to sub-degree, and accuracies range from hundreds of micrometers to tens or even single micrometers. It is clear that having an FSM is a common choice amongst these types of applications. The mechanism to drive the FSM varies, but many devices have space heritage already.

To come to a final conclusion on a design, it is important to define a set of requirements that the device must fulfill. This list of requirements is summarized in Table 3.1 and discussed in detail below.

In order for the FPU to be effective, it must be able to correct pointing errors up to the level of the coarse pointing system. This will dictate the field of view the FPU will be required to achieve. Different satellite buses offer different accuracies in pointing that vary from $\sim 10^\circ$ to $< 0.01^\circ$ [152]. The finer pointing accuracy, the higher the cost of the bus as well as the requirement for more sensors. For instance, some of the less accurate

Title	Requirement	Reference
Field of View	The field of view shall be at least ±0.3°	[146]
Pointing Accuracy	The pointing accuracy shall be at least ±20 µrad	[147]
Tracking Loop Bandwidth	The tracking bandwidth shall be able to compensate ±0.3° at 1 Hz and ±0.03° at 20 Hz	[148]
Collinearity	The collinearity of the quantum link and beacon link shall be within 5 µrad	[147]
Polarization	The entire channel shall not cause a polarization error >4°	[149]
Beacon sensitivity	The system shall function for an input beacon power from 0.05 µW to 10 µW	[150, 151]
Long-term fluctuation sensitivity	The beacon detector shall accommodate a 10 dB slowly varying dynamic range over 100 s	[150, 151]
Link induced detector fluctuation sensitivity	The beacon detector shall be able to accommodate a minimum 10 Hz to 100 Hz signal fluctuation of at least 10 dB from min to max	[150, 151]

Table 3.1: The major requirements needed for a proper implementation of an FPU. These requirements stem from previous studies as well as published in a QKD satellite link analysis paper [89].

satellites use simply magnetometers. To become more accurate, the satellite must include star trackers, Earth trackers, sun sensors, and/or other devices. A typical Earth-sensing satellite can achieve accuracies on the order of 0.5°, such as the NEMO-AM [146], with ±0.3° within reach. The field of view requirement for this project was determined to be ±0.3° as it was deemed feasible for a satellite bus to achieve coarse pointing accuracy to this level. This selection was also chosen taking into account systems, cost and complexity.

The pointing accuracy of 20 µrad is a requirement on the device as referenced in the call from the Canadian Space Agency (CSA) [147]. This requirement also stems from the field of view of the IOA that is to be mounted onto the back of the FPU. This device has four multi-mode fibers where the collected light must enter, and determines the requirement for the overall pointing precision.

The bandwidth requirement follows from jitter caused by the satellite. Even though a satellite moves through essentially a vacuum, it still has internal jitter caused by its movement mechanisms, such as reaction wheels. This will not only cause vibrations locally around the wheels, but depending on the size, shape, and material of the satellite, it may cause further vibration effects across the entire satellite. Jitter has been studied [148] and it has been determined that a majority of the jitter is at low frequencies, often less than

1 Hz. There are very minor effects at higher frequencies, but having a tracking bandwidth of 20 Hz for lower vibrations can readily combat this issue.

The collinearity of the beacon and the quantum link applies to within the FPU, and implies that the deviation between where the beacon signal is measured on the position sensitive device should correspond to the deviation of the quantum signal entering the IOA, to within 5 µrad. Again, this is a specification within the call for project proposals initiated by the CSA [147].

As the quantum signal encodes the quantum key information in the photon polarization, it is important to ensure that this information can be correctly analyzed (in the IOA) and is not altered by the FPU. There are other places where the polarization can be effected, such as the ground optics, the transmission link, the receiver telescope, but these are not of concern here except that the entire channel can only implement 4° of total error as explained below. Fortunately the ground station can compensate for much of its own unitary polarization transformations before sending the photons, and photon propagation through the atmosphere is known to have negligible effect on polarization [153–155]. As a goal, it would be beneficial if the FPU could attribute <1° error in the polarization, leaving budget for other components.

To help quantify the quality of polarization preservation, the visibility between the two polarizations in a given basis can be measured. Based on previous experience, we assume that the reduction from an ideal visibility of 100 % should be no more than 1 %. This can be calculated by

$$V_{HV} = \frac{|I_H - I_V|}{I_H + I_V} \geq 0.99, \tag{3.1}$$

for an ideal H or V input state, where I_H and I_V are the measured intensities of the horizontal and vertical polarizations. This should also hold for the states in any other relevant basis (diagonal and anti-diagonal, in our case).

One issue which could arise is the issue of the frame of reference between the transmitter and the receiver. If the receiver is rotated at a nonzero angle, θ, relative to the transmitter, the basis will not be perfectly aligned and polarization error will enter the system. Neglecting other effects, the intensities of the two states of a basis, as measured at the receiver, follow $I_{H/D} \propto \cos^2\theta$ and $I_{V/A} \propto \sin^2\theta$, given an H or D input, and from there it can be found that in order to keep $V_{HV/DA} \geq 0.99$, the angular deviation must be less than approximately 4°. This drives the overall requirement for polarization error.

Different materials in mirrors can have different effects on the P and S polarizations of light reflecting off of them. One effect can be a different reflectivity. If a diagonal state,

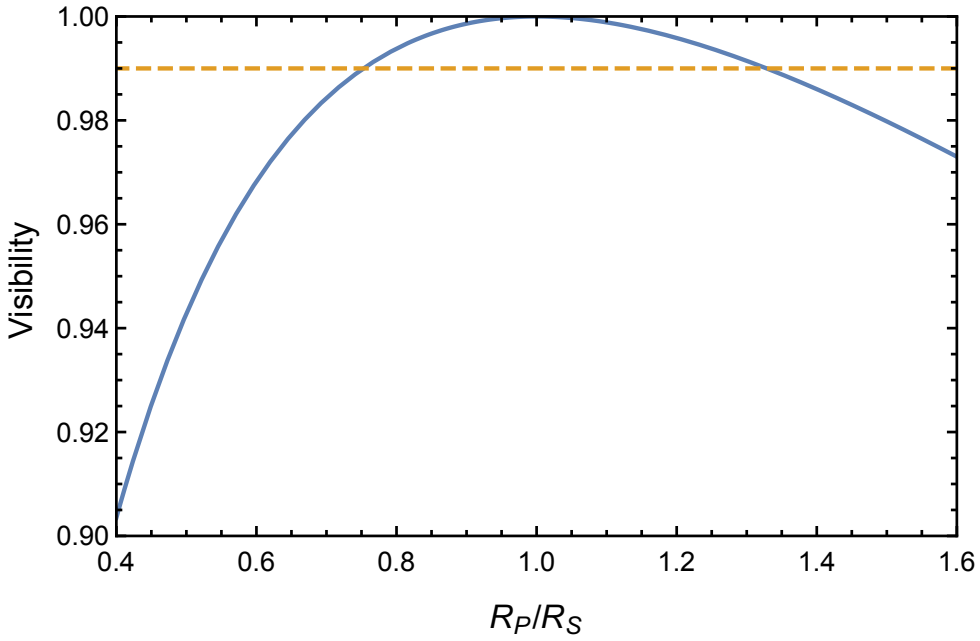


Figure 3.1: Visibility as a function of the ratio of reflectivity of the P polarization to reflectivity of the S polarization. The dotted line signifies the 99 % visibility requirement.

written in ket notation $|D\rangle = (|H\rangle + |V\rangle)/\sqrt{2}$, is reflected off a mirror with reflectivity R_P and R_S aligning to H and V respectively, the output state can be given as

$$|D'\rangle = \frac{\sqrt{r}\,|H\rangle + |V\rangle}{\sqrt{r+1}}, \tag{3.2}$$

where r is R_P/R_S. The visibility of the state as a function of the ratio r is illustrated in Figure 3.1.

A mirror may also impart a phase onto one polarization with respect to the other. Again with a diagonal input, state the output state can be written as

$$|D'\rangle = \frac{|H\rangle + e^{i\phi}\,|V\rangle}{\sqrt{2}}, \tag{3.3}$$

where ϕ is the phase between H and V polarization states (P and S). The effect of this phase shift can be seen in Figure 3.2.

Another risk is the effect of an incoming beam with an angular spread. As different parts of the beam reflect from the mirror, their polarizations will be affected differently, which can cause a depolarization of the beam as a whole. The optical elements which the beam reflects from must also be analyzed to determine if they impart any phase on the reflected light.

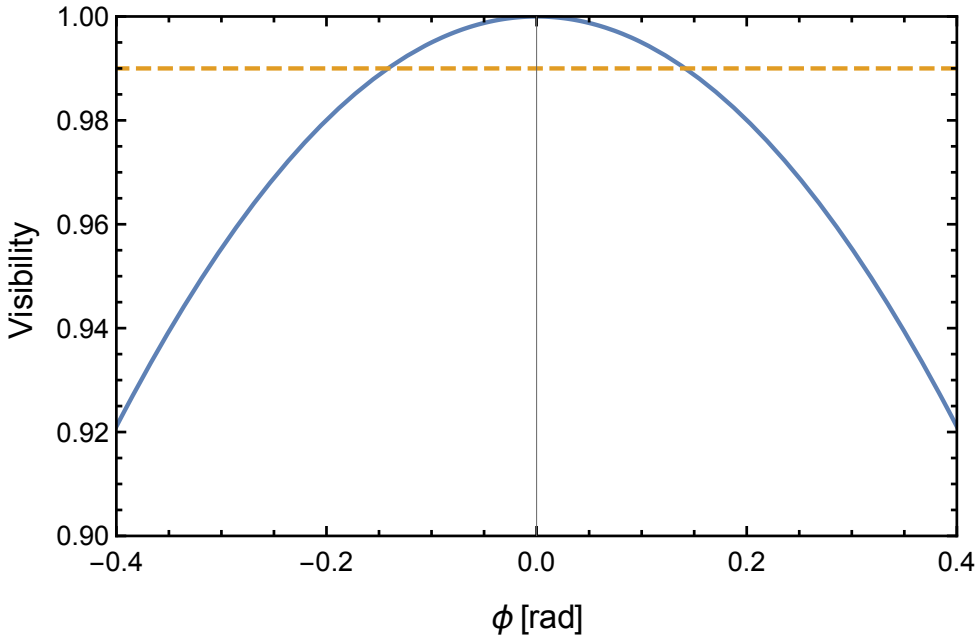


Figure 3.2: Visibility as a function of the phase ϕ between the P polarization and the S polarization. The dotted line signifies the 99 % visibility requirement.

As the beacon beam propagates through the atmosphere to the satellite, it will experience atmospheric turbulence, diffraction, atmospheric absorption, and pointing errors. This is especially important in the up-link as the atmosphere appears in the beginning portion of the propagation and a large angular disturbance is caused early on creating a larger beam at the end compared to a down-link, causing greater loss. This effect has been studied experimentally in [150, 151].

Three effects happen as the beacon propagates through the atmosphere—these will relate to the last three requirements in Table 3.1. The first of these effects is loss due to the factors mentioned above. The beacon signal received by the FPU will thus be significantly weaker than what is sent. This loss can vary significantly depending on the angle of elevation and the pointing error. We have theoretically modeled this loss—an example, under certain conditions, can be seen in Figure 3.3.

The second effect is that of scintillation caused by turbulence in the atmosphere. This effect will cause intensity fluctuations of the beacon signal which peak at just below 100 Hz [151]. Fluctuations also occur at lower frequencies, but tend to fall off sharper for higher frequencies. This means the beacon detector must be able to cope with signal intensity fluctuations on the order of 100 Hz. These fluctuations tend to be approximately 10 dB in magnitude.

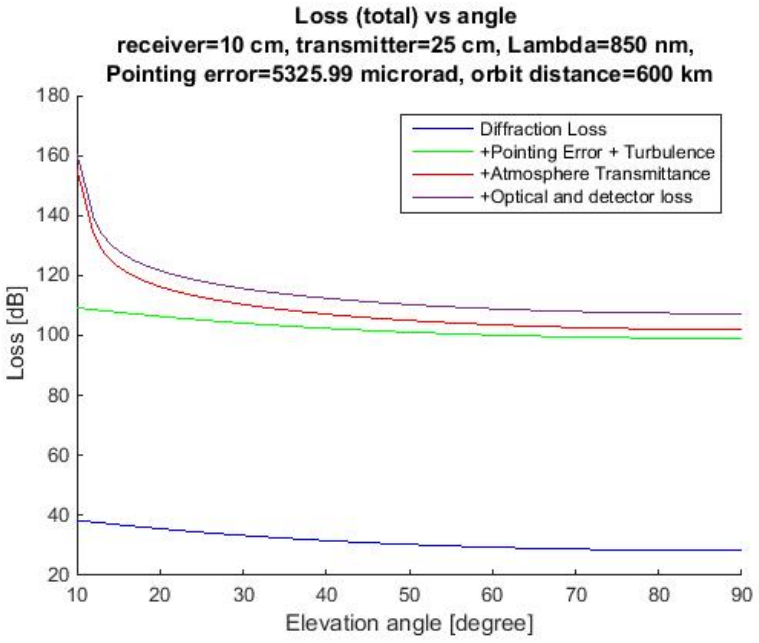


Figure 3.3: Theoretical beacon loss to a satellite orbiting at 600 km. The atmospheric model is of sea level with rural-5 km visibility. The pointing error is approximately 0.3° and the optical loss is 3 dB. The detector efficiency is 59 %.

The last effect which will be experienced is a slow variation in beacon intensity on the position sensitive detector due to the movement of the satellite. When the satellite rises over the horizon, the beacon received will have low power due to the longer distance traversed through space and atmosphere. As the satellite nears zenith, the beacon power will increase in average intensity. The beacon detector must be able to accept a reasonable range of beacon intensities which are expected to slowly vary over the time of a satellite pass.

A detailed design analysis and trade-off study was conducted with INO, and a tip-tilt mirror design was chosen for its space heritage, as well as the availability of commercial FSM components. A schematic of the design proposed by INO can be found in Figure 3.4. This design uses a tip-tilt mirror configuration for beam steering with collimation and correction optics for the beam coming from the telescope. Only the first tip-tilt mirror is necessary, the other piezo mirror is for gross beam stabilization, is not necessarily required, and will not be used in this particular implementation. An additional lens would also be required to focus the light coming from the FPU system into the IOA.

The moving mass in this system is very little, which is good for limiting vibrations of the system. It will be important to choose an appropriate location for the tip-tilt mirror in

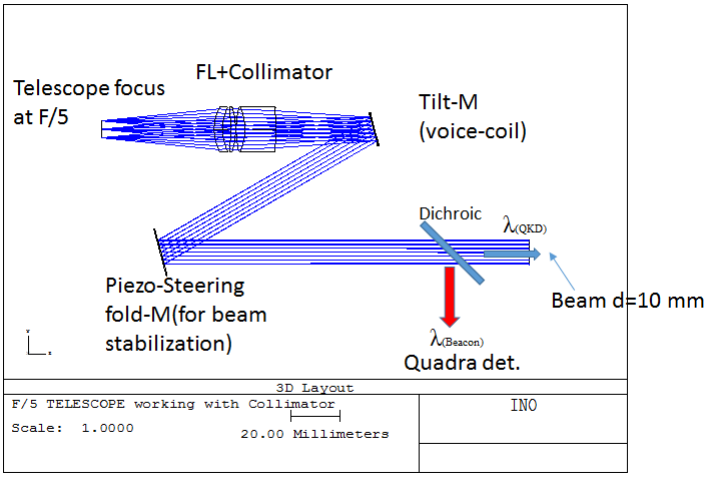


Figure 3.4: Schematic of FPU designed by INO, using a tip-tilt mirror to steer the beam. Since the beam entering the system will be collimated, polarization issues can be reduced from reflections, although further study is still required. (Figure produced by INO)

the setup to provide the necessary pointing accuracy and polarization preservation, which was studied by INO, since two mirrors will be used. The purpose for the folding mirror is for space considerations in the use of the device in prototype models.

When not operating, the FPU should ensure that the beacon spot hits the surface of the quad detector. That way the device will always have the ability to track as long as the beacon is entering the telescope (at an angle less than the field of view). The incoming beam to the FPU is collimated, which will help eliminate problems from an angular beam spread.

3.3 Design

There are two key components to the design of the FPU: the optical portion, and the control portion, both of which are described below.

3.3.1 Optical Portion

The optical portion of the FPU was designed by INO and uses a tip-tilt mirror for the correction of the beam wander. The quantum and beacon signals each enter from the telescope which is attached to the front of the FPU. The telescope used for this project was the Tele Vue-NP 101is (focal length, f=540 mm, aperture, D=101 mm). The collimation

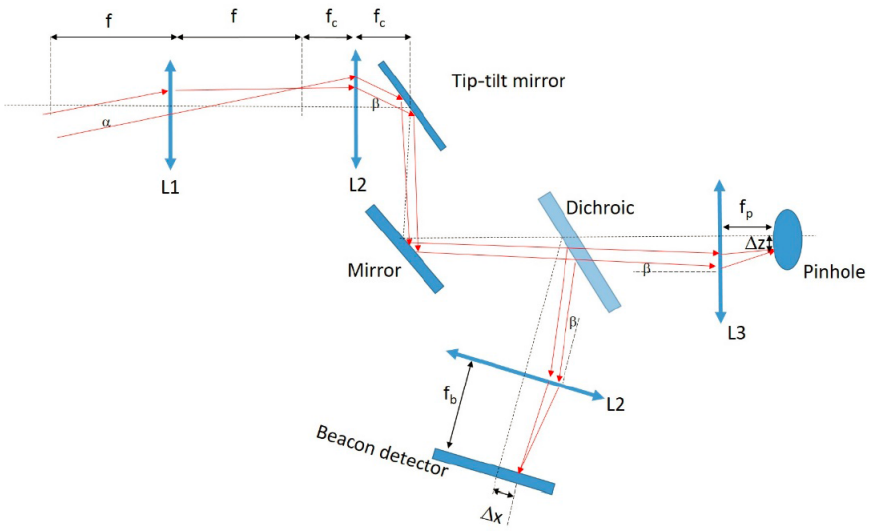


Figure 3.5: Optical design by INO for the FPU. L1 is the telescope objective lens, the first L2 in the optical path indicates the beam collimation optics, the second L2 is the lens to focus the beacon beam onto the quad detector (Beacon detector in the image), and L3 is the lens to focus the quantum beam into the pinhole. The FPU will start at the first L2 and end at L3. Note: Filters not included in this schematic. (Figure produced by INO)

optics at the entrance to the FPU collimate the light from the telescope so the beam is collimated as it propagates through the FPU. This lens assembly can be adjusted in position to allow for collimation. Figure 3.5 shows a schematic drawing provided by INO for the FPU.

After the light from the telescope is collimated, the beam reflects off a tip-tilt mirror (OIM101 from Optics in Motion) which is used to steer the beam, and another folding mirror which is fixed. The tip-tilt mirror uses voice coils to move the mirror, which have been used previously in space applications (although not for this particular model). The fold mirror can be easily removed so the beam can exit the FPU enclosure and be checked for collimation at this point. A dichroic mirror then separates the quantum and the beacon signals, with the quantum beam being transmitted and the beacon beam being reflected. The quantum beam then passes through optical filters and is focused onto the 50 µm pinhole in the IOA. The filters are housed in a tray which is removable, and up to three one-inch-diameter standard-thickness filters can be placed in this tray. For the planned use of this device, two 785 nm central wavelength, 3 nm bandpass filters were used. The IOA is mounted on the back of the FPU with custom adapter plates. The beacon beam is focused onto the quadrant detector (QD). The beacon wavelength used is 850 nm and a 850 nm

central wavelength, 10 nm bandwidth filter is used to isolate the QD from background light.

When the system is in the neutral position, the beacon signal should be located in the center of the QD and the quantum signal should be in the center of the pinhole. When the incoming light is input at an angle, α, this will cause a shift of Δz away from the center of the pinhole and Δx away from the center of the QD. To assess the performance of the FPU, we must know the deviation from the center of the QD as a function of the input angle. This can be shown to be

$$\Delta x \approx f_b \left(\frac{f\alpha}{f_c} \right), \tag{3.4}$$

where f_b is the focal length of the beacon focusing lens (60 mm), f is the focal length of the telescope (540 mm), and f_c is the effective focal length of the collimation optics (66 mm).

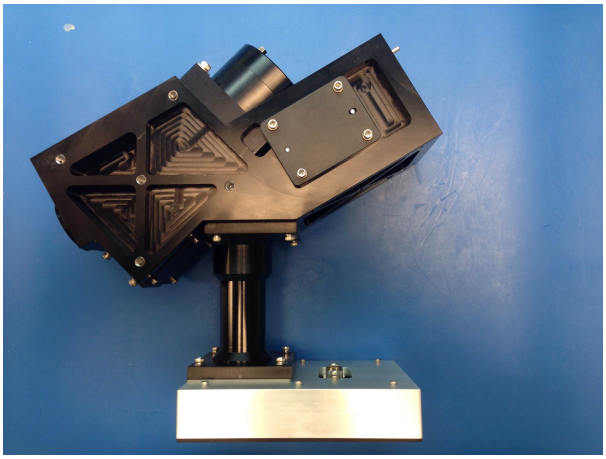
Custom mirror coatings were also developed by INO in order to maximize reflectivity and minimize polarization error for 785 nm.

The metal casing for the optical portion of the FPU was built from an aluminum alloy, with certain parts being Invar 36 to ensure temperature stability when sensitive alignment is required. This can be seen in Figure 3.6(a). The total mass of this portion is 2.42 kg, excluding the mass of the IOA.

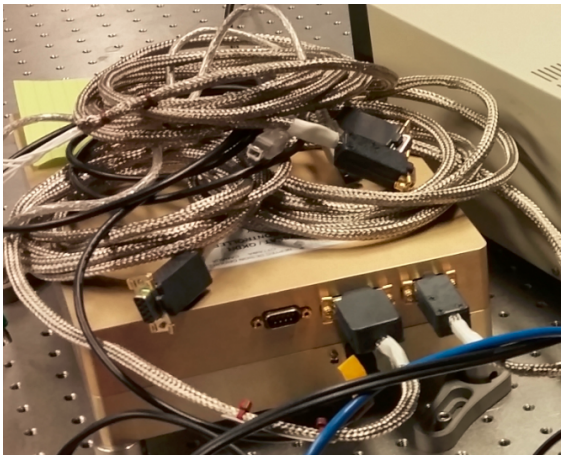
3.3.2 Control Portion

The control portion of the FPU consists of three parts: the QD card (provided by INO), the QD interface card, and the FSM interface card. The system performs closed-loop tracking using the signal from the QD to control the position of the tip-tilt mirror. This portion of the project was designed and implemented by Neptec Design Group.

The QD card consists of the QD, trans-impedance amplifiers which convert the quadrant signals into voltages, and voltage amplifiers which provide the sum and error voltages. The QD interface card provides the power conversion from 28 V unregulated (a common voltage supplied by satellite buses as well as stratospheric balloon systems) to the proper voltages for the device. It also has variable gain amplifiers to amplify the sum and error signals from the QD card. There is also an automatic gain control circuit to maintain the sum signal output at constant amplitude. The FSM interface card provides analog to digital conversion of the quad sum and error signals. It then uses a field programmable gate array (FPGA) signal processing loop to determine the correction which is needed by the tip-tilt mirror to move the beacon spot to the center of the quad sensor. Finally it has digital to



(a)



(b)

Figure 3.6: (a)The optical portion of the FPU. The beam enters from the left and the tip-tilt mirror actuator can be seen at the top of the image. The gray box at the bottom is the QD and the QD card. The IOA and IOA adapter plates are not attached in this image. (b) The controller box with the cable connection ports (facing the front). The cables on top extend to the QD card, the tip-tilt mirror, and the power source.

analog converters for converting the signals which are sent to the tip-tilt mirror, as well as the power driver circuits for the mirror.

Two of the three cards (the QD interface card and the FSM interface card) are housed in a metal enclosure with input ports for power and for the signal from the QD card, an output port for the tip-tilt mirror cable, and a USB port for control and monitoring of the unit. This unit, along with the accompanying cables, weighs 4.32 kg and can be seen in Figure 3.6(b).

3.4 Performance

The first step before the FPU was tested was to mount it onto the Tele Vue telescope. This was done with a custom adapter and rails for stability. The FPU was attached to the rails with sliders which allowed the telescope focus to move in and out to ensure the FPU was in the correct location with respect to the focal point of the telescope. This setup can be seen in Figure 3.7.

There were four phases of testing to determine the functionality of the device and to make sure it performed properly in different scenarios. Phase 1 determined some of the

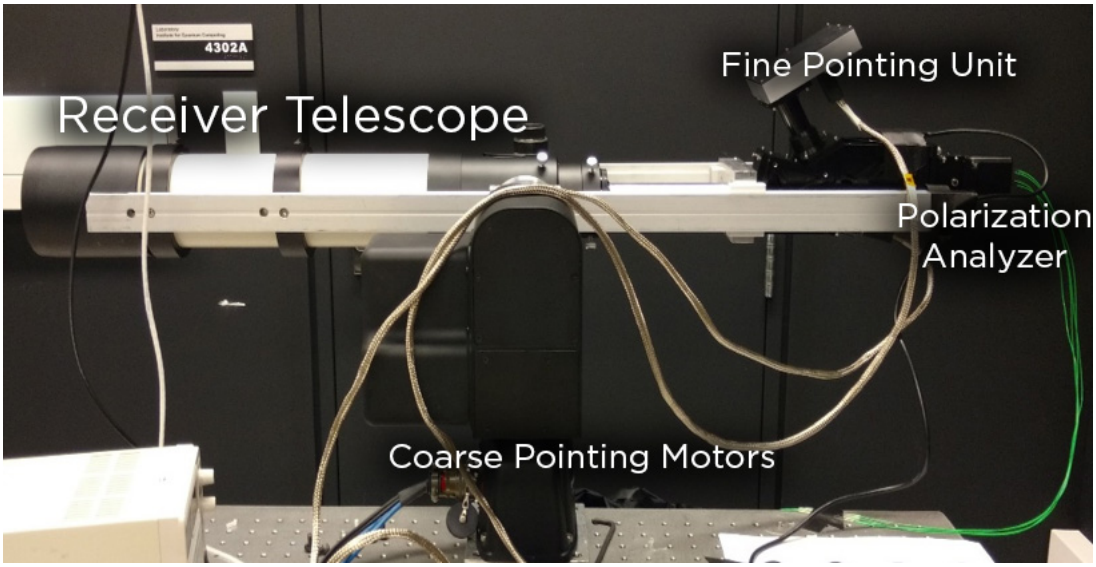


Figure 3.7: The FPU is mounted onto the back of the telescope with a custom adapter and rails for stability. The IOA is mounted onto the back of the FPU and the four fibers (carrying the four measured polarization states) can be seen draping down to the right. The entire assembly is mounted onto a motor assembly which allows for movement.

basic features of the device such as mass, volume, and light-tightness. Phase 2 saw signals injected into the FPU and measured parameters such as transmission, polarization effects, and field of view. Phase 3 is where QKD was performed in various orientations with the system stationary. Phase 4 is where the system was moving while performing QKD.

For Phases 2-4 the optical signals to test the FPU were generated by either a strong polarized laser at 785 nm or a WCP source (described in Chapter 5). The power at the transmitter was monitored using a fiber beam-splitter with one output connected to the transmitter (previously characterized for loss) and the other port connected to a power meter. The ratio of the fiber beam-splitter was known, so by reading the power meter, the ratio could be applied and the power being transmitted could be found. This method was only used for the strong laser as the WCP source power is measured in a different way. The transmitter also incorporates a polarization compensation system (described in Chapter 5) for the QKD signals, to compensate for any drift in polarization from the fibers while the photons propagate to the telescope from the source.

A beacon laser at 850 nm was reflected off a mirror which was mounted in a stage with a piezo slab and then coupled into a fiber. The piezo slab could be modulated and provide a difference in coupling efficiency, thus changing the output power of the beacon signal. The beacon was then combined with a fiber combiner and sent through a telescope towards

the receiver telescope, to which the FPU was attached

3.4.1 Phase 1

The purpose of phase 1 was to determine some basic features of the device such as mass, dimensions, light tightness.

The mass of the FPU, including the IOA attached, was measured to be 7.13 kg including the control portion, the optical portion, and cabling. The volume, as it would appear if it were a box, would have dimensions of $33 \times 24 \times 9.5$ cm for the optical portion and $33 \times 24 \times 8$ cm for the control portion. The mass and volume were chosen to be below threshold values based on common satellite bus requirements given by the CSA. A total allotment of 10 kg and $50 \times 50 \times 25$ cm was given to the FPU, which the designed unit fell within as the two portions of the FPU could be separated.

It is important that very little to negligible stray light be able to enter the system so as to avoid noise in the QKD signal. The light tightness of the FPU was tested by using a bright flashlight and illuminating various parts of the FPU while measuring the output of the four output fibers of the IOA on single-photon detectors. The IOA and fibers were covered using black optical cloth as these portions were designed separately and are known to not be light tight. The measured increase of light was on the order of several hundred to a few thousand photons which translates to a suppression of approximately 150 dB, demonstrating very little stray light entering the system. The device also turned on and we were able to operate it with the graphical user interface (GUI) and text-based software provided by Neptec.

3.4.2 Phase 2

The second phase involved no active coarse pointing, and the motors were moved manually to align the telescopes. The system was placed on a FLIR motor mount (seen in Figure 3.7) which includes encoders allowing for the readout of the positions of the motors. This motor system was controlled through software for the alignment and step movements. The setup for this phase can be seen in Figure 3.8. This phase measured the transmission, field of view, as well as polarization effects from the FPU.

The transmission of the FPU was measured by sending the signal laser through the system from the transmitter and measuring the output of the four fibers with a power meter. After factoring out the transmission loss from the filters and the IOA (measured previously), the transmission was determined to be 89.7%.

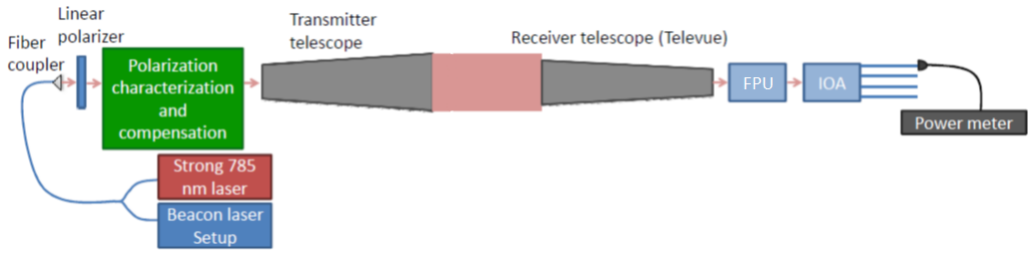


Figure 3.8: The Phase 2 setup, where a strong 785 nm laser was polarized and used to measure various characteristics. The receiver telescope was mounted on a FLIR pan-tilt motor mount but was moved manually as no active movements were engaged at this time. Either a power meter or a single-photon detector were used to detect the signals.

It was also important to measure the transmission of other wavelengths through the system to determine if they would contribute to the noise. Measurements of the other wavelengths were done with single-photon detectors as the signals were too weak to register on a power meter. For 850 nm (the beacon wavelength) the single-photon count changed little with 1.6 µW (6.8×10^{12} photons/sec) entering the FPU, showing greater than 120 dB suppression. When 532 nm light was used, a count rate increase of 566,720 counts/sec was measured with an input power of 24.8 µW (6.7×10^{13} photons/sec), yielding a suppression of 80 dB. Finally, 662 nm light was used and with an input of 760 µW (2.54×10^{15} photons/sec), there was an increase of 333,262 counts/sec, which is a suppression of 98 dB.

To measure the field of view of the system, FPU tracking was initiated and the system was moved horizontally and vertically until the tracking stopped working in both directions. The field of view of the horizontal axis (as defined from the lab frame with the QD at the top) was found to be $\approx \pm 0.65^\circ$ and in the vertical axis it was $\approx \pm 0.55^\circ$. The system was required to have at least a $\pm 0.3^\circ$ tracking range, and exceeded this.

In order to determine the effect on polarization from the FPU, a linear polarizer was placed at the transmitter before the telescope, and a set of wave-plates was used to rotate the polarization to the six states H, V, D, A, R, and L. Each polarization output of the IOA was then measured with a power meter. The FPU system was turned on and the coarse motors were used to move the telescope to various positions. If the FPU perfectly preserves polarization, the expectations would be as shown in Table 3.2 for each input (ignoring the imperfections of the IOA). We will only ever have 50% output from the same polarization because of the 50:50 beam-splitter which selects between the two bases in the IOA.

Table 3.3 shows the results for beam coming into the center of the field of view. Figure 3.9 shows the results with various input polarizations and the measured outputs for all of

	H [%]	V [%]	D [%]	A [%]
H	50	0	25	25
V	0	50	25	25
D	25	25	50	0
A	25	25	0	50
R	25	25	25	25
L	25	25	25	25

Table 3.2: The percentage of received power of each of the four output polarizations expected for different input polarizations.

	H [%]	V [%]	D [%]	A [%]
H	0.1	50.1	26.1	23.6
V	48.1	0.4	23.4	28.1
D	21.4	27.9	8.4	42.2
A	26.9	22.3	42.3	8.5
R	24.8	24.4	6.8	44.0
L	20.5	28.7	43.3	7.5

Table 3.3: The percentage of received power of each of the four output polarizations from the IOA for different input polarizations. This measurement was for the center of the field of view.

the measured positions (the position index can also be found in Table 3.4). The values presented show the percentage or received input, *i.e.* the four polarization outputs are summed and the value of each polarization is divided by that total.

From the measurements, the first clear observation was that the opposite of what was expected was occurring for the orthogonal polarizations. This was due to a 90° rotation between the transmitter reference frame and the receiver reference frame. This caused no problems with using the system as the polarizations can be somewhat arbitrary in their definition, as long as the relative difference remains the same.

The measurements across the field of view show that the D and A polarizations are not maintained through the system. Fortunately this effect was a constant rotation across all positions in the field of view. Since this was the case, it could be corrected by a constant phase offset, allowing the proper states to be received by the system. (It had been identified that the coating of the dichroic mirror was the cause of this phase offset—a new coating was designed, and a new dichroic with this coating has been procured.) The largest variation

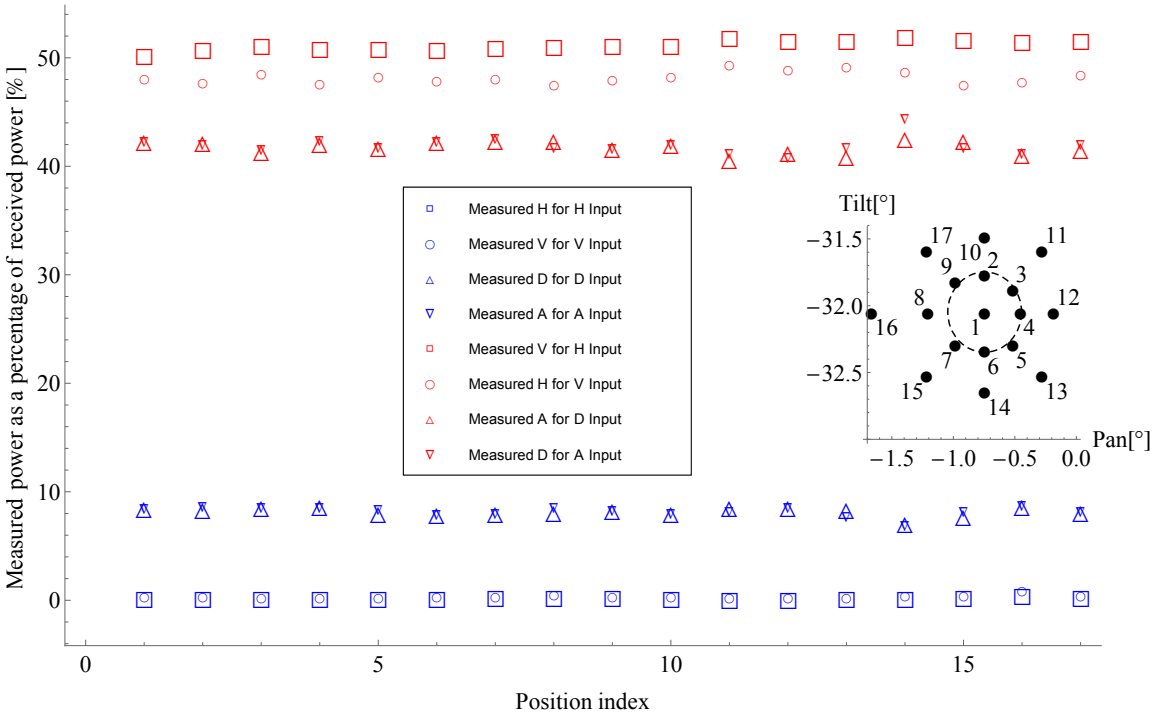


Figure 3.9: Output polarization as a percentage of input polarization for the four states H, V, D, and A. The inset plot shows the position of the FLIR pan-tilt mount for each measurement. The dotted circle in the center is the required 0.3° field of view.

Pos [#]	Pan [°]	Tilt [°]
1	−0.746	−32.047
2	−0.746	−31.769
3	−0.515	−31.879
4	−0.453	−32.047
5	−0.515	−32.287
6	−0.746	−32.337
7	−0.983	−32.287
8	−1.205	−32.047
9	−0.983	−31.819
10	−0.746	−31.484
11	−0.278	−31.585
12	−0.184	−32.047
13	−0.278	−32.524
14	−0.746	−32.639
15	−1.217	−32.524
16	−1.664	−32.047
17	−1.217	−31.585

Table 3.4: Position index and the corresponding pan and tilt locations.

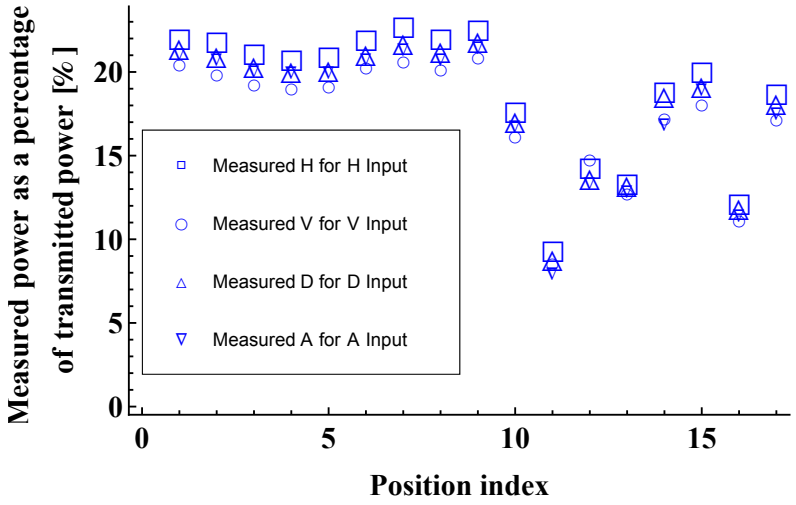


Figure 3.10: Received power as a percentage of transmitted power for various positions around the field of view. The positions are the same as for Figure 3.9. The loss includes the free-space channel, both telescopes, the FPU, and the IOA.

of any of the polarization measurements across the field of view was 3.6% which was within the measurement uncertainty of this procedure. The values measured in Table 3.3 were the values used to optimize the correction at the polarization compensator on the transmitter for the future phases.

The polarization transmission measurement was also used to verify the change in total transmission of the unit with positions. The four polarizations H, V, D, A were sent in and the total power out was measured as a function of transmitted power. The losses include the free-space channel, both telescopes, the FPU and the IOA. The results can be seen in Figure 3.10.

It was noticed that there was a drop in transmission near the edges of the measured range and further tests were performed to verify that this 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 $\pm 0.7^\circ$ from center), the QD 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 FWHM of the signal coupling efficiency distribution was measured. In all cases, it was observed that the coupling efficiency remained constant over most of the width, only dropping when near the edge. This was consistent with a focused signal spot size being 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

		Center Position [µm]		FWHM [µm]	
Pan [°]	Tilt [°]	x	y	x	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

Table 3.5: Measured center and width of the coupling efficiency distribution.

the beam begins to be clipped by the pinhole. A drop in coupling efficiency due to varying collinearity would require a change in the center position that is significant compared to the width (e.g., a change in the center position which is half the width would be required to reduce the coupling efficiency by 50%.) The results of the measurement are shown in Table 3.5.

In all cases, the change in the center position (compared to the central position of pan $= -2.0195° \pm 0.006°$, tilt $= -3.949° \pm 0.006°$) was 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 the X center (26 µm) and more than six times the largest change in Y center (22 µm). This implied 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. 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.

3.4.3 Phase 3

The third phase involved no active coarse pointing, as with Phase 2, and the motors were moved manually to align. The setup for this phase was similar to that in Figure 3.8. However, the strong 785 nm laser was replaced by the WCP source, and the power meter was replaced by four single-photon detectors. The system performed QKD and the QBER, key generation rate and final key were monitored for different positions of the coarse motor (corresponding to the various mirror positions as shown in the inset of Figure 3.9) to ensure successful key generation.

Figure 3.11 shows the QBER, average count rate, and secure key after 100 s of data collection for each of the mirror positions. Post-processing steps (error correction and

privacy amplification) were also performed on each data set. Every position was able to generate over 10 kbit, with the largest secure key length being 116 kbit. The average loss measured during these tests was 36 dB to 39 dB, most of which was artificially added by decoupling connected fibers in order to prevent the saturation of the detectors, and because these were typical loss values expected for the satellite concept.

The QBER varied between 2.89 % ± 0.2 % to 3.66 % ± 0.2 % across all the positions. This variation could be explained by fluctuations in the QKD source, indicating that the polarization effect of the FPU was constant and could be pre-compensated by adding a constant phase to the transmitted signals. The count rate was also observed to drop as the outer positions were reached, which was consistent with the transmission drop near the outer positions as seen in the previous phase. The lower secure key comes directly with this reduced count rate as there the influence of finite-size statistics takes a stronger effect.

3.4.4 Phase 4

The final phase tested QKD performance while the receiver coarse motors were moving. The setup is the same as for Phase 3 except for the movement of the motors. Various movement scenarios were designed to test the FPU under different conditions. The first portion of the moving tests consisted of oscillation at 1 Hz and in the x-direction, y-direction, diagonally or in a circle with 0.3° amplitude (the intended field of view of the FPU). The diagonal oscillation went through the center of the field of view to the two corners, and the circular oscillation rotated around the center of the field of view.

To simulate atmospheric turbulence causing intensity fluctuations in the beacon beam, the beacon laser was also modulated in amplitude at either 10 Hz or 100 Hz. The average power, with these modulations, was either 50 nW or 7.4 µW and they were fluctuated by either 10 dB or 20 dB in all combinations, which were typical ranges expected for the QEYSSAT mission.

The system also was required to be tested at a higher frequency of movement of 20 Hz, but unfortunately the coarse motors could not oscillate at this frequency. To test this, step movements were performed over 0.5° at a speed of $3.77\,^{\circ}\,\mathrm{s}^{-1}$ which would correlate to a sinusoidal motion of 0.3° amplitude at 20 Hz. The count rate and pointing data were analyzed over this step to detect if there was a drop in performance.

During each of the movements and beacon oscillation trials, QKD data was recorded for 100 s. The known polarization problem from the dichroic was pre-compensated at the transmitter side.

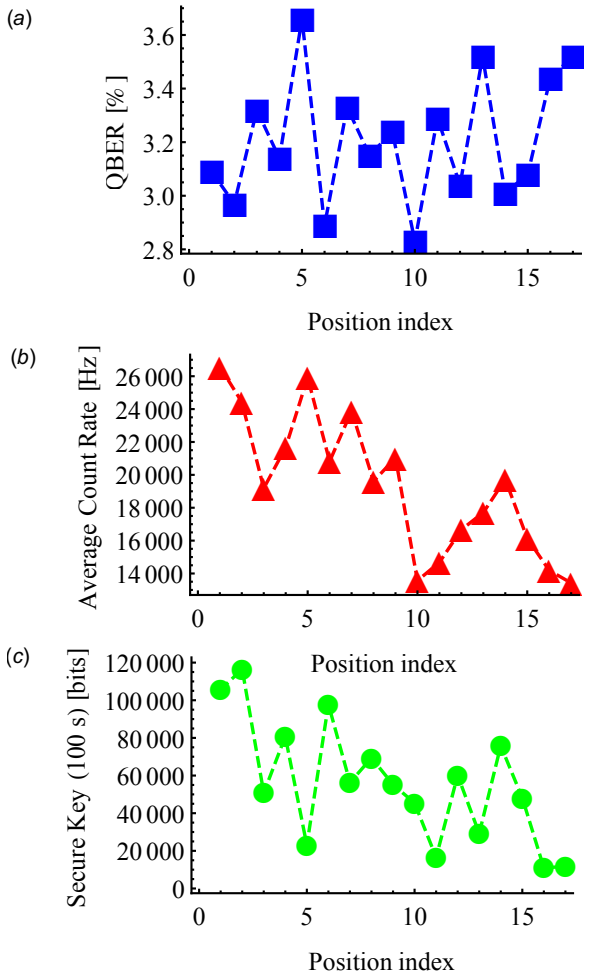
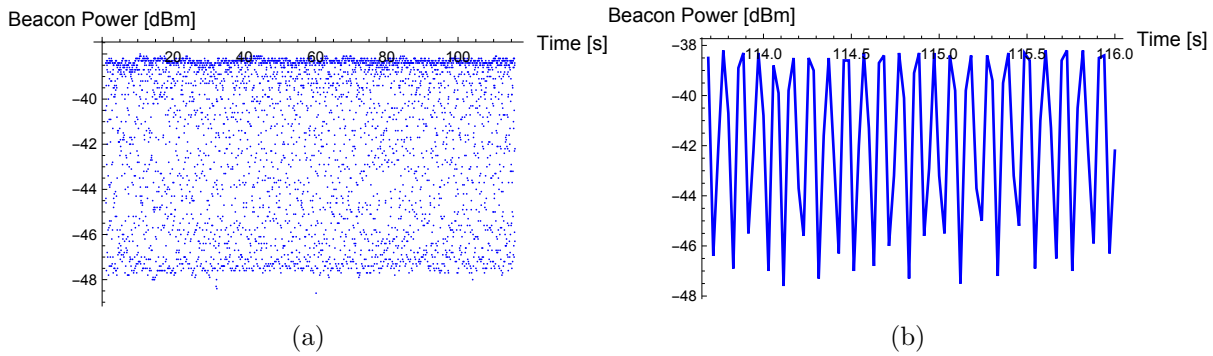


Figure 3.11: All data was taken over 100 s and the positions map to those shown in the inset of Figure 3.9 in Phase 3. (a) Average QBER, which varies from 2.89 % ± 0.2 % to 3.66 % ± 0.2 %, within the natural fluctuation range of the QKD WCP source. (b) Average count rate for the various positions. As the unit reaches the edges, the average count rate drops as performance at the edges is not as ideal as in the center. (c) Final secure key. The final secure key takes, QBER, average count rate, and many other parameters into account.



(a) (b)

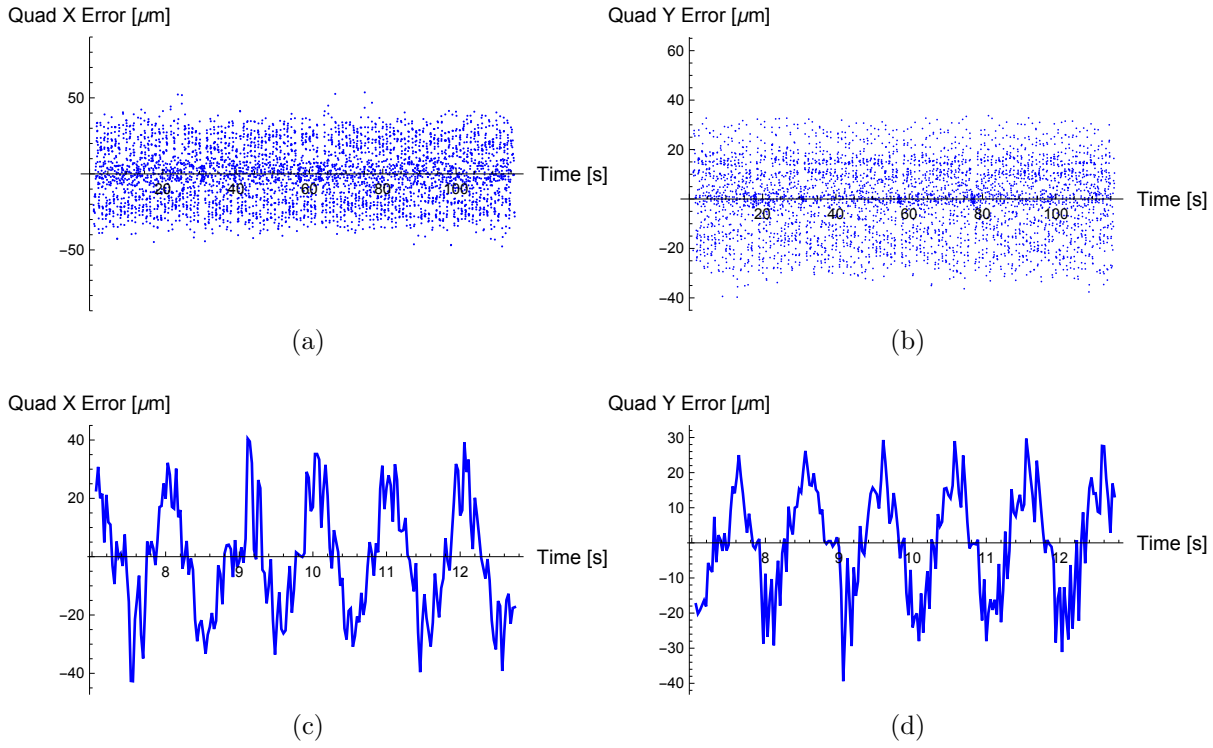
Figure 3.12: (a)Beacon power measurements while the beacon was being modulated at 10 Hz and fluctuating 10 dB in power. The measurement is sampled at approximately 35 Hz. (b)Zoom in view near the end of the sample with the points connected by lines, showing the approximate sine wave reconstruction. The minimum power measured over this run was −48.2 dBm and the maximum power measured was −38.1 dBm.

The FPU control software records the beacon power, x-position on the QD, y-position on the QD and time stamp at a rate of approximately 35 Hz (there were slight variations across the 100 s and this was taken into account for the analysis) into a text file. Before the QKD protocol was initiated, the motors were started in their movement pattern, the beacon laser was modulating and the FPU was initiated. Once all the systems were turned on, the QKD protocol was started and ran for 100 s and then stopped. Separate files were generated for each run and a sample of this data is shown here. Post processing was not calculated for the QKD data in this section due to time constraints, but the estimated final key is reported.

The beacon intensity was modulated via a sine wave analog control through the piezo slab. Figure 3.12(a) shows the beacon power over a run with a modulation of 10 Hz and 10 dB in power fluctuating with an average power of 50 nW. Figure 3.12(b) is a zoomed in view of the same data with the connected samples showing the approximate reconstruction of the sine wave modulation.

Figure 3.13 demonstrates the x and y positions of the beacon spot on the QD (x and y errors) over time for a diagonal movement of the coarse motors. From this data, the mean error for both the x and y directions was calculated as well as the standard deviation. These values for all the different combinations of motor movements and beacon fluctuations can be found in Tables 3.6 and 3.7.

The mean values of the x and y direction errors should be 0 µm in the ideal case. For a majority of the combinations of motor movements and beacon fluctuations, this was



(a) (b) (c) (d)

Figure 3.13: The motors were moving diagonally with an amplitude of 0.3°. The beacon was fluctuating at 10 Hz with an amplitude of 10 dB m with an average power of approximately 50 nW. (a)The error in the x-direction as measured on the QD. (b)The error in the y-direction as measured on the QD. (c)Zoomed in view of the error over approximately 7 s in the x-direction. (d)Zoomed in view of the error over approximately 7 s in the y-direction.

x **Mean Spot Error** [µm]/ y **Mean Spot Error** [µm]	Beacon Variation and Power					
	10 µW		50 nW			
Motion	10 dB 10 Hz	10 dB 100 Hz	10 dB 10 Hz	10 dB 100 Hz	20 dB 10 Hz	20 dB 100 Hz
Vertical Line	−0.023/ −0.37	0.0044/ −0.065	0.032/ −0.17	−0.0057/ −0.0056	0.30/ 2.02	0.045/ 0.021
Horizontal Line	0.016/ 0.010	−0.20/ −0.0098	0.20/ 0.0059	−0.12/ 0.015	1.37/ −0.11	−0.079/ −0.031
Diagonal Line	−0.025/ 0.037	0.031/ −0.018	−0.084/ 0.067	0.016/ −0.021	0.79/ 0.89	0.030/ −0.031
Circle	0.039/ −0.13	0.070/ 0.12	−0.19/ 0.016	0.15/ −0.023	2.88/ 0.17	−0.11/ −0.13

Table 3.6: Mean x and y spot errors on the QD measured during various motor movements and beacon fluctuation scenarios. Many of the trials show a mean very close to 0 µm, as should be the case. The values in the 5th column are slightly higher, which can be attributed to the beacon drop out as the power went below the threshold measurement of the device.

approximately the case. For the circumstance where the beacon had an average power of 50 nW and the beacon was fluctuated at 10 Hz over 20 dB, it was noted that the mean errors deviated from 0 µm. This can be attributed to the beacon signal being lost and erroneous signals being measured during these times. The device had a low power threshold around 10 nW and the power was frequently below this in these trials.

For an idealized device without bandwidth limitations, , one would expect a standard deviation of the pointing error to be zero. In reality, this is not the case and there will be an error. In all of the trials, if the motors were not moving in a specific direction, the error was usually <5 µm. In the cases where the motors were moving in a particular direction, the standard deviations of the errors were typically around 25 µm. Using equation 3.4 this error corresponds to an angular error of ≈50 µrad. In the case where the average power was 50 nW and the modulation was 20 Hz over 20 dB, the errors can again be seen to be quite higher than the other trials, again due to the loss of signal at the lower threshold and the erroneous QD positions measured at these times.

We performed QKD during these movement trials to determine if secure key could be generated. Table 3.8 shows the QBER for each of the various scenarios. The QBER was shown to be similar for all tests with minor fluctuations which are within the natural fluctuations of the source. This is very positive, as the active tracking appears to have

x **Error Standard Deviation** [µm]/ y **Error Standard Deviation** [µm]	Beacon Variation and Power					
	10 µW		50 nW			
Motion	10 dB 10 Hz	10 dB 100 Hz	10 dB 10 Hz	10 dB 100 Hz	20 dB 10 Hz	20 dB 100 Hz
Vertical Line	3.85/ 22.35	3.93/ 22.34	3.91/ 22.51	3.98/ 22.65	9.82/ 51.38	4.94/ 22.63
Horizontal Line	25.45/ 1.76	25.72/ 2.07	25.53/ 1.77	25.91/ 1.84	66.38/ 16.81	25.64/ 1.97
Diagonal Line	18.93/ 14.98	18.90/ 14.96	18.73/ 14.55	18.89/ 14.58	37.61/ 30.52	18.90/ 14.83
Circle	25.79/ 22.55	29.02/ 30.92	26.09/ 22.41	26.04/ 22.37	73.72/ 71.69	22.46/ 22.41

Table 3.7: Standard deviations of the x and y spot errors on the QD measured during various motor movements and beacon fluctuation scenarios.

negligible results on the errors observed in the QKD protocol.

The average count rate, as shown in Table 3.9 did vary somewhat between the different trials. This was mainly noticed when the power of the beacon dropped below the threshold of detection and therefore the signal was lost. The average count rate measured when the motors were not moving was ≈36,000 counts/s. Table 3.10 shows the predicted secure key after 100 s. As with the count rate, the tests at 50 nW with 10 Hz over 20 dB fluctuation showed a significant drop. All tests performed showed a predicted key rate above 80 kbit, with only two tests predicting below 100 kbit.

The full QKD protocol post-processing (to extract the actual secure key) was only performed on one test (circular motion, at 50 nW with 10 Hz and 20 dB variation), as this trial predicted the lowest secure key length of all the tests. The error correction efficiency used to estimate the key generated was taken from Phase 2 and was the worst case scenario error correction efficiency for runs with similar QBER. Since the worst case scenario error correction efficiency was used in the calculation, the predicted key length is likely to be an underestimate of the actual key which could be generated. The loss during the tests in this phase averaged 35 dB, which was less loss than introduced in Phase 2 and therefore allowed higher key rates and secure key lengths.

The step movements to test the device with faster movements (20 Hz) were performed on all six beacon modulation scenarios as described in the tables above, but only the count rates and tracking statistics were recorded. This was done because all previous tests showed that the FPU did not significantly impact the QBER and that the main effect to the secure

Signal QBER [%]	Beacon Variation and Power					
	10 µW		50 nW			
Motion	10 dB 10 Hz	10 dB 100 Hz	10 dB 10 Hz	10 dB 100 Hz	20 dB 10 Hz	20 dB 100 Hz
Vertical Line	3.6	3.3	3.1	3.5	3.6	3.7
Horizontal Line	3.8	3.3	3.2	3.5	3.6	3.7
Diagonal Line	3.6	3.4	3.4	3.5	3.6	3.7
Circle	3.4	3.3	3.4	3.5	3.7	3.7

Table 3.8: The average QBER during the QKD protocol while the tracking was active for various scenarios. The QBER did not change significantly over any trial which shows the active tracking of the device to have negligible impact on the QBER during the QKD protocol. The uncertainty in the QBER was 0.2 %.

Average Count Rate [Hz]	Beacon Variation and Power					
	10 µW		50 nW			
Motion	10 dB 10 Hz	10 dB 100 Hz	10 dB 10 Hz	10 dB 100 Hz	20 dB 10 Hz	20 dB 100 Hz
Vertical Line	36968	36751	36531	34175	32781	36524
Horizontal Line	34892	38938	36661	35431	28905	37068
Diagonal Line	36104	36680	37771	36783	33498	37785
Circle	35613	35255	35874	36096	28779	34985

Table 3.9: The average count rate for various active tracking scenarios. The count rate remained fairly constant during most tests, averaging 35,461 counts/s, very close to the average count rate measured when the motors were not moving of 36,370 counts/s. Only the run with 50 nW, 10 Hz and 20 dB fluctuations showed a large deviation due to the loss of signal during these trials. There were also some source power fluctuations during these specific runs.

Key in 100 sec [bits]	Beacon Variation and Power					
	10 µW		50 nW			
Motion	10 dB 10 Hz	10 dB 100 Hz	10 dB 10 Hz	10 dB 100 Hz	20 dB 10 Hz	20 dB 100 Hz
Vertical Line	124,600	159,158	149,251	182,253	92,542	118,621
Horizontal Line	103,378	153,139	156,709	175,561	131,570	128,762
Diagonal Line	148,853	136,154	120,576	198,478	151,483	157,327
Circle	144,946	187,751	152,924	131,918	89,618	166,659

Table 3.10: Predicted secure key lengths for the various active tracking scenarios. The predicted key length was over 80 kbit for all tests, averaging 142 kbit. Only during the 50 nW, 10 Hz and 20 dB fluctuating trial predicted less than 100 kbit due to the reduced count rate from the loss of signal and the lower source power during these tests.

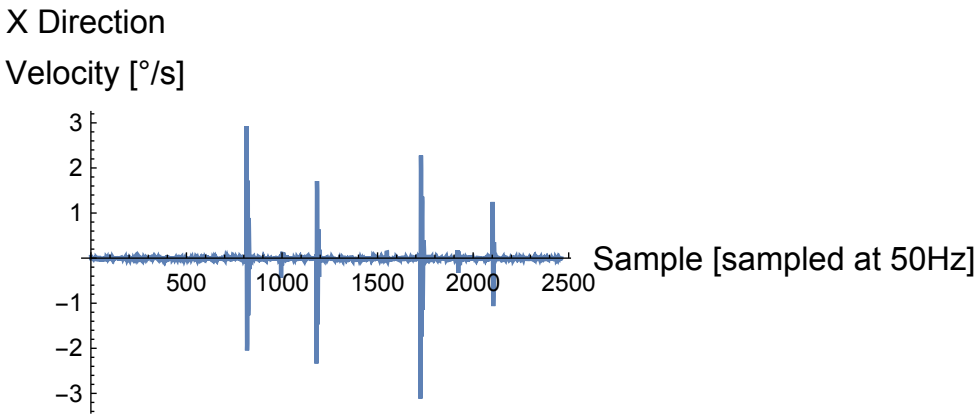
key length was the count rate.

There were a total of seven one-shot movements per trial, which moved by alternating vertical and horizontal movements in squares around the center position. A Vectornav VN-300 attitude sensor was mounted onto the FPU to record its movement, sampled at 50 Hz, as the motors moved. This allowed us to record the angular speed at which the entire device moved for analysis. The movements as recorded by this device can be seen in Figure 3.14. With the plots on top of each other, the alternating pattern of horizontal and vertical movements can be clearly seen over time.

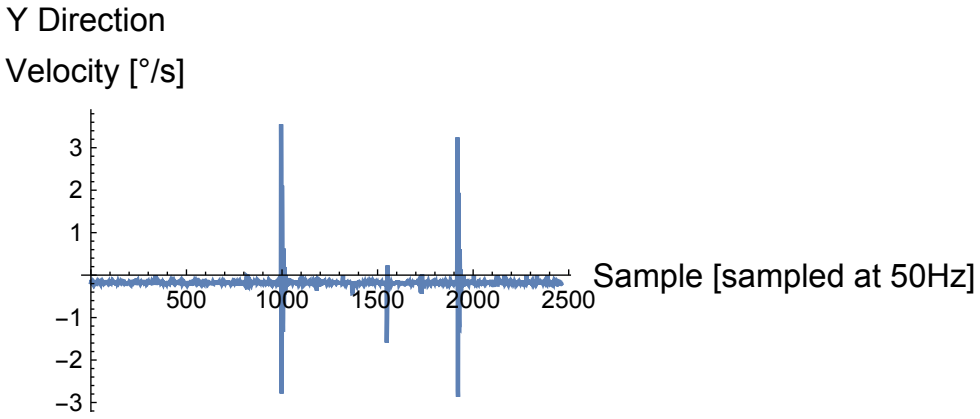
The beacon spots as recorded on the QD for the various step movements can be seen in Figure 3.15. The movement seen at the beginning of the time period was the motors being reset from the previous test. The seven horizontal and vertical movements can then be seen starting just after 10 s.

The velocity was analyzed during each of the one-shot movements and the accumulated sum was calculated to find how far the device had moved during that time period. Figure 3.16 zooms in on the first peak movement in the vertical direction. This particular peak reached a maximum of 3.73 °/s.

The motors initially moved the system to 0.128° in 40 ms as calculated from the velocity information and knowing that the system was sampled every 20 ms. This would average to moving 0.064° in 20 ms which would correspond to a single-shot movement on the order of 0.06° at 50 Hz. This movement can be seen in Figure 3.17. The system also shows movement back in the opposite direction and oscillations as the system tries to settle on 0.05° and the system vibrations dampen.

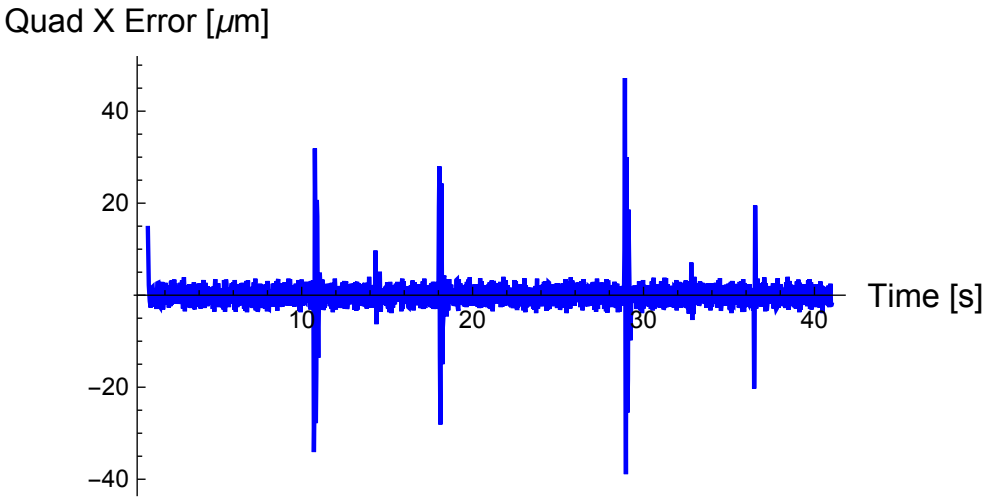


(a)

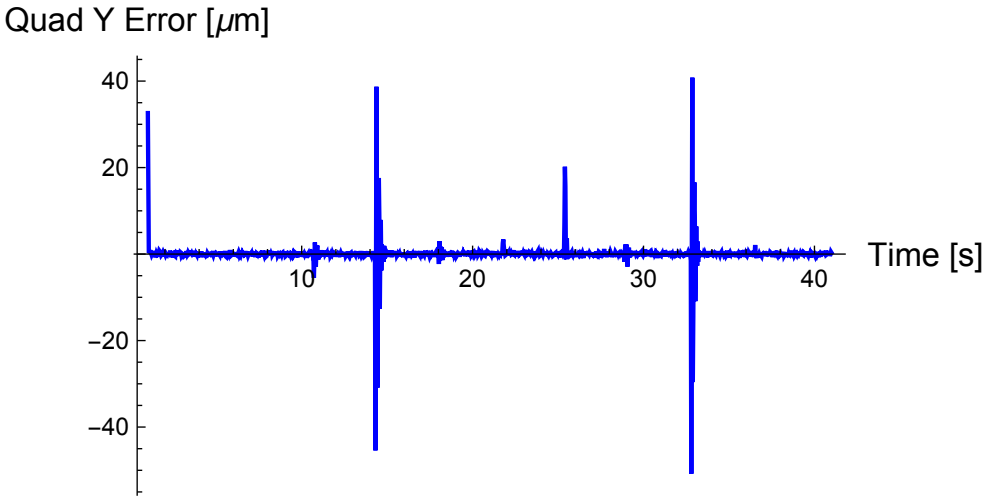


(b)

Figure 3.14: Angular velocity measurements recorded by the VN-300 for both the (a)horizontal and (b)vertical directions. The device sampled the movements at 50 Hz. Each of the spikes corresponds to a one-shot movement of 0.05°. There appeared to be an offset from zero when the device was not moving in the y-direction, but this was normalized out for the analysis. A magnification of the first peak in the y-direction can be seen in 3.16.



(a)



(b)

Figure 3.15: Beacon spot position on the QD for both the (a)horizontal and (b)vertical directions. Each of the spikes corresponds to a one-shot movement of 0.05°.

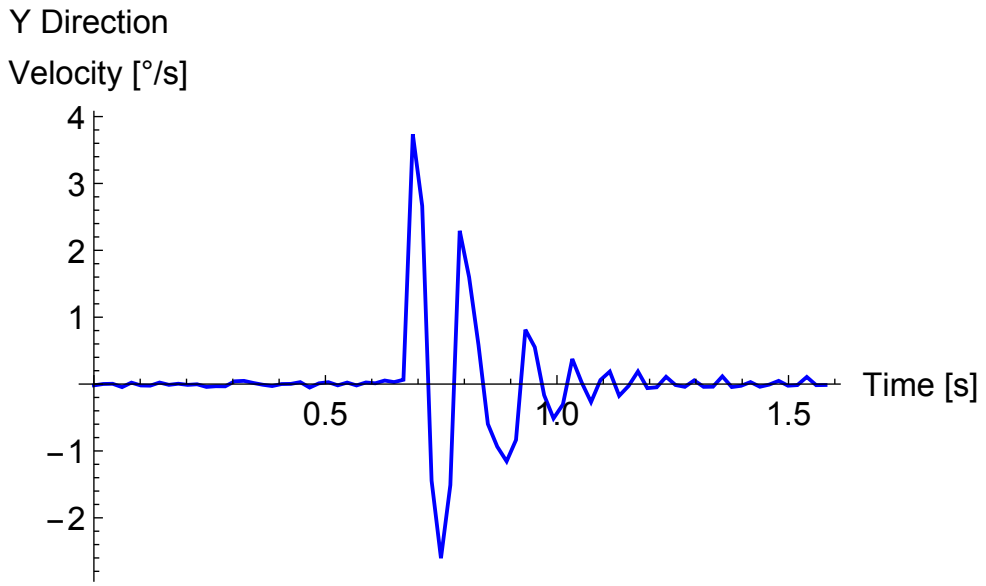


Figure 3.16: The initial movement of the motors, as well as oscillations and system flexure to achieve the final position of 0.05°. The peak velocity of the motors is 3.73 °/s.

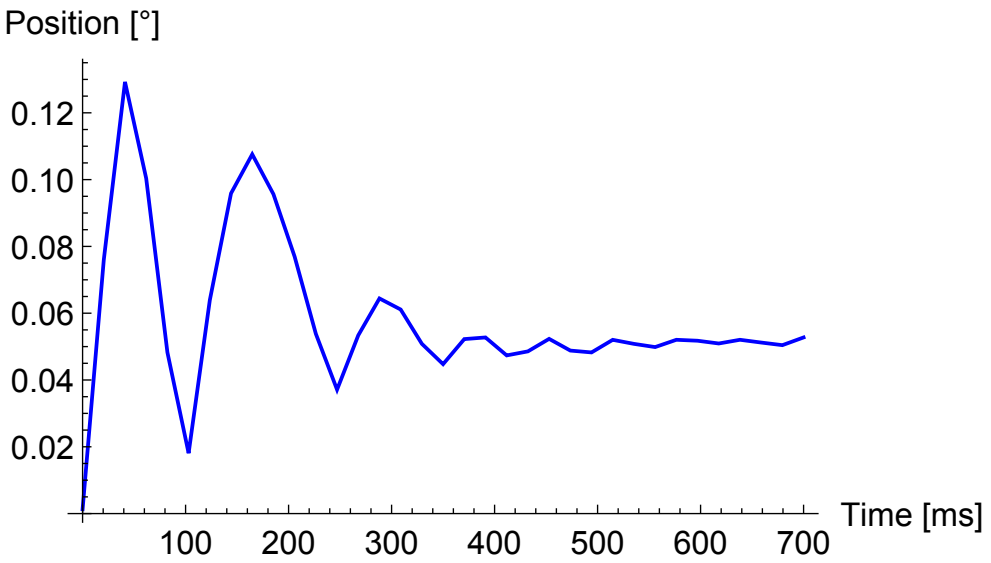


Figure 3.17: Calculating the position of the one-shot movement based on the velocity measured by the VN-300. The system reached a peak distance of 0.128° in 40 ms, which when averaged corresponds to a movement of 0.06° at 50 Hz.

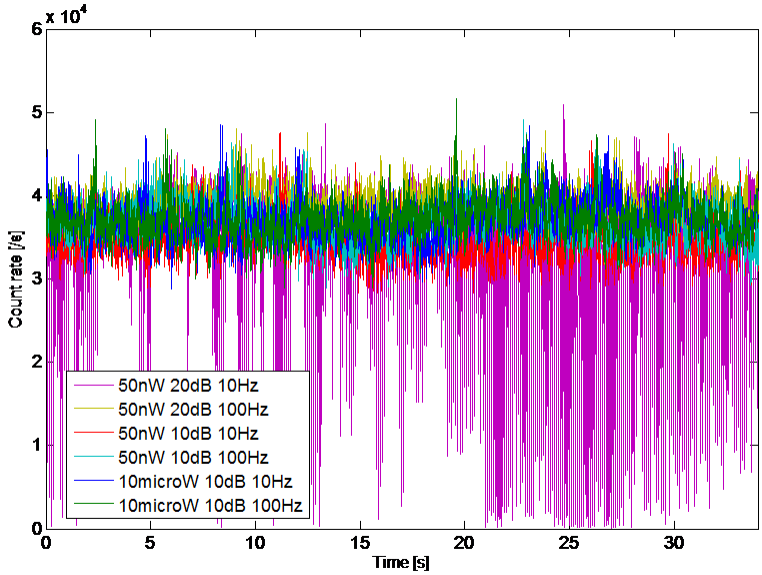


Figure 3.18: Received count rate per second during the one-shot movements for each of the beacon fluctuation scenarios. Only one of the trials showed drop-outs of signal (20 dB at 10 Hz with a maximum of 50 nW), which shared the period of the laser modulation. This was due to the beacon signal dropping below the threshold of detection of the QD and the mirror returning to the center position. All other trials show no drop in signal during any of the one-shot movements, of which there were seven per trial.

In order to determine if the system is able to handle these quick movements, the received count rate is analyzed in blocks of 10 ms (and for plotting purposes, renormalized to counts/s). Figure 3.18 displays the various trials, and shows there is no decrease in count rates at any time with one exception. The counts for the beacon modulation of 20 dB at 10 Hz showed drops in counts occurred periodically, which can be attributed to the loss of signal when the beacon power went below threshold.

The periodic drop-out can be seen better in Figure 3.19. It is clear that the drop out is occurring at 10 Hz frequency, which was the beacon laser modulation frequency. The power dropped to ≈4.3 nW, below the 10 nW threshold. All the other beacon modulation situations showed a received count rate that remained stable within normal signal fluctuation. If the FPU system had not been able to follow the movement, it would be expected that there would be a noticeable drop in count rate corresponding to the instances where the motors were moved (seven times per each test). Since the count rate was analyzed in blocks of 10 ms and the first peak movement was measured to last 40 ms, a drop lasting around 4–5 points would have occurred. In all tests, there was no evidence of a drop

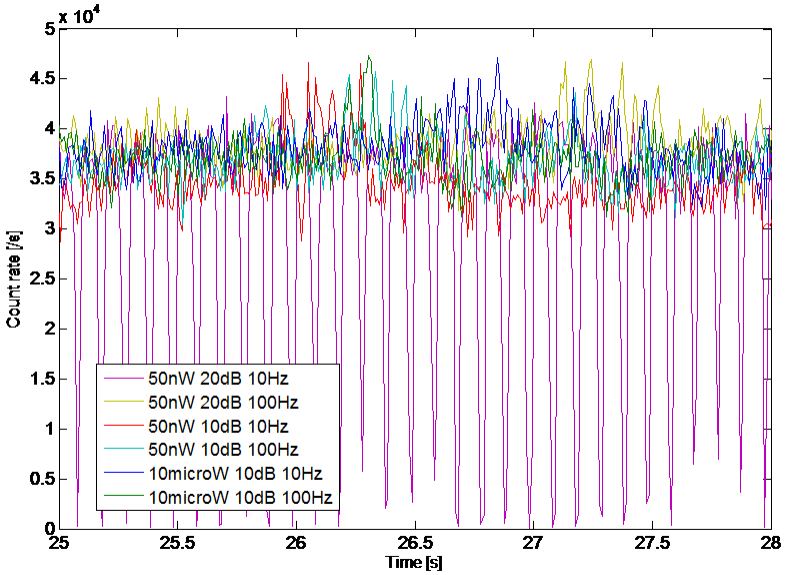


Figure 3.19: Received count rate per second during the one-shot movements for each of the beacon fluctuation scenarios, zoomed in over 3 s. Only one of the trials showed a drop-out of signal (20 dB at 10 Hz around 50 nW) which was periodic with the period of the laser modulation. This was due to the beacon signal dropping below the threshold of detection of the QD and the mirror returning to the center position. All other trials show no drop in signal during any of the one-shot movements of which there were seven per trial.

in signal due to the step movements. The brief drops did not occur where the beacon modulation was fluctuating at 20 dB around 50 nW at 100 Hz because the time where the beacon signal was below the threshold of the quad sensor was too short for the system to lose signal and move back to the central position (estimated at 3.9 ms, as compared to 39 ms with the 10 Hz modulation).

The system was also tested for a slowly varying intensity, as will be experienced as a satellite passes over a ground station. For these trials, the beacon power was modulated at 0.01 Hz over a 10 dB range with an average power of 112 nW, and over a range of 30 dB around 214 nW. The beacon power over time can be seen in Figure 3.20. As with the one-shot measurement, only the count rate and pointing data were collected.

These trials were performed with the coarse motors moving with a circular motion of 0.3° amplitude at 1 Hz. The pointing performance for the trial around 112 nW can be seen in Figure 3.21. The pointing performed similarly to the previous trials showing a mean spot error around 0 µm and a standard deviation around 25 µm.

The received count rate remained stable through these trials within normal signal fluc-

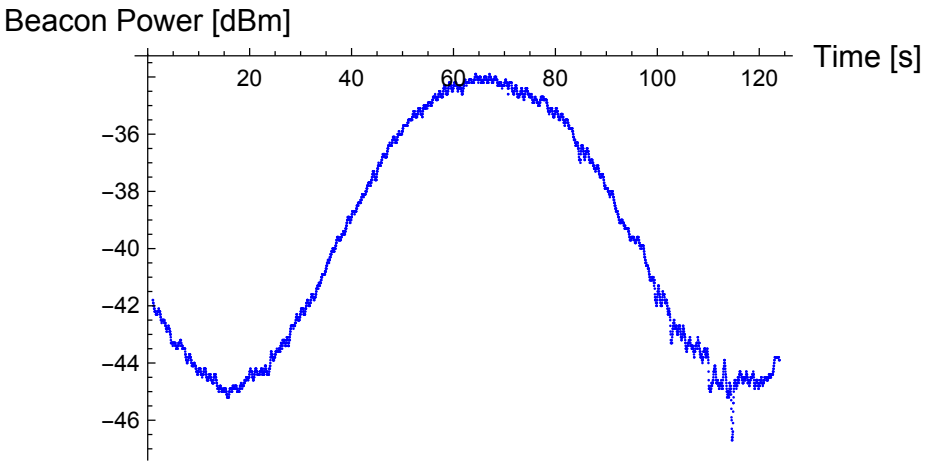
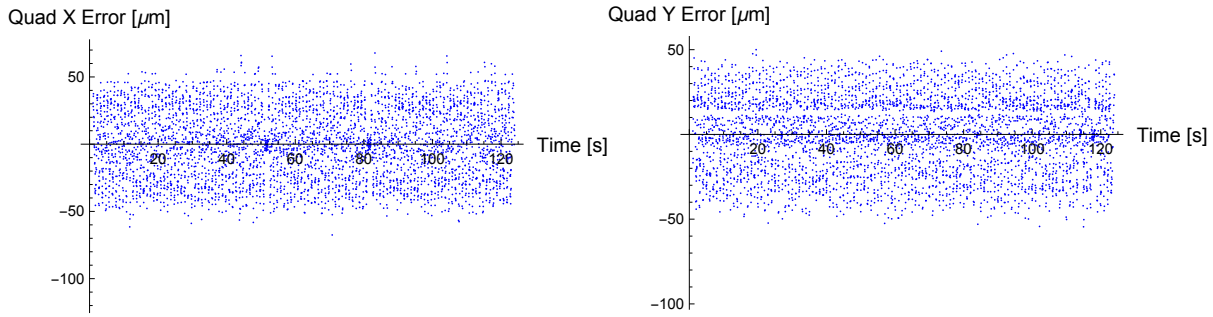


Figure 3.20: The beacon was varied at 0.01 Hz over 10 dB with an average power of 112 nW. This was to test the slowly varying power which would be experienced as a satellite passed over a ground station.



(a) (b)

Figure 3.21: The coarse motors were moving in a circle with an amplitude of 0.3°. (a)The x-error had a mean spot position of $-0.021\,\mu\text{m}$ and the standard deviation was $26.27\,\mu\text{m}$. (b)The y-error had a mean spot position of $-0.040\,\mu\text{m}$ and the standard deviation was $22.46\,\mu\text{m}$. These results are similar to those for faster beacon modulation.

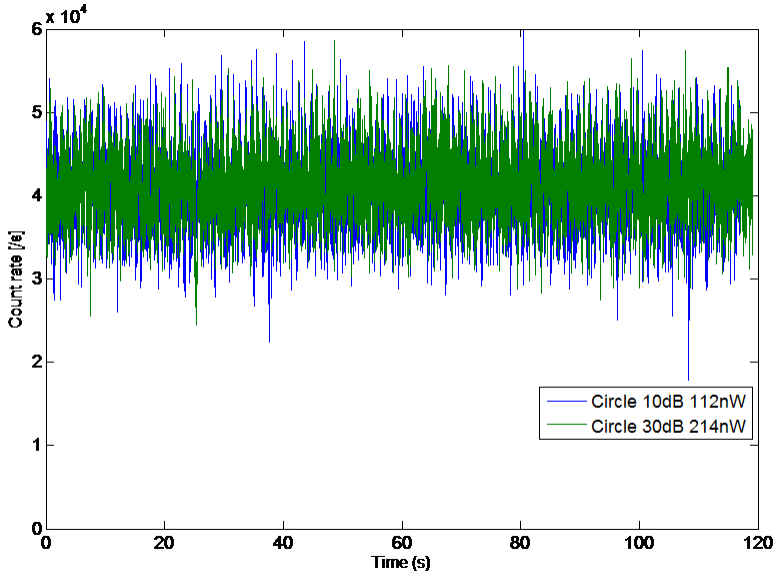


Figure 3.22: Received count rate as the beacon power was slowly varying by 10 dB around 112 nW and by 30 dB around 214 nW at 0.01 Hz.

tuation, showing no evidence of a drop out. The count rate can be seen in Figure 3.22.

3.5 Discussion

In order to determine the usefulness of the device which has been designed and tested, it is important to compare it against the design requirements as defined in Table 3.1.

The measured field of view of the device, where the tracking was still functional and quantum secured key could still be extracted, was $> \pm 0.5°$ in both directions, which exceeds the target requirement of $\pm 0.3°$. This relaxes the requirement on the open loop tracking of the satellite bus which could help reduce cost.

Although the FPU measured accuracy of 50 µrad did not meet the required 20 µrad accuracy, the design and implementation could be optimized, especially in the control circuit design, and given further study, will be reimplemented with circuitry to meet the requirement. The measured accuracy will work for closer range tests (∼10's of kilometers) but will need to be upgraded for a satellite implementation (∼600 km).

Testing the unit under 0.3° amplitude, 1 Hz movement showed positive results and the system was able to generate key while these movements were happening. Since we were limited in our ability to shake the unit at 20 Hz, we tested the unit with step movements

and compared the maximum speed achieved and the distance moved during that time to determine the unit could correct for movements at approximately 50 Hz, as no drop in signal was observed during these movements.

The collinearity between the signal and the beacon could not be precisely determined, but was deemed to be aligned well enough to allow the successful operation of the device. The focused spot size was much smaller than the pinhole so the alignment allowed for the beam to go through the pinhole while scanning over the whole field of view.

The dichroic mirror which caused the phase offset in the diagonal polarization channel will be replaced in case a polarization pre-compensation system is not available, which should bring the overall polarization error to a tolerable level for QKD.

Testing various fluctuation and power levels of the beacon ensured that the QD and tracking algorithms were able to perform under a scintillating free space link. The device performed better than the requirements and was able to perform with fluctuations of up to the tested 20 dB magnitude as long as the power level did not go below of the bounds of the detector sensitivity. Section 4.4 shows results for the first time the device was taken outside and used in an outdoor free space link.

One of the important aspects of this device is the path to space flight. For the optical portion of the device, the mechanical design uses materials that have space heritage and are suitable for sensitive optical systems (*i.e.*, rigid). All of the lenses are bonded with a very low out-gassing silicone, which is an important factor in space suitability. The current FSM in use is not itself space certified, but there are similar counterparts which do have space heritage and these options are to be studied in future work. Other components such as the QD must also reach space certification, but again, similar space qualified counterparts exist.

Many of the circuits within the electronics controller already have space heritage, and the remaining ones that do not have fairly clear alternatives that could be used instead. The size and weight of the device is also under consideration—the controller box can certainly be halved in both size and mass.

3.6 Conclusion

We built and demonstrated a fine pointing system which is suitable for QKD. This system was demonstrated in the lab and able to perform tracking easily up to 50 Hz vibrations as well as lower frequencies while preserving the polarization of the photons. The accuracy of

the system was approximately 50 µrad and the constant polarization phase shift was easily corrected. The next steps for this device will be to test it over free space channels outdoors and on moving targets. The components have a clear and identified path to flight, making the transition to a satellite-suitable version possible and reasonably straight forward.

Chapter 4

Preparation for Airborne Tests of Quantum Key Distribution

Notes

Parts of this chapter are adapted from material published on June 6, 2017 as [156]:

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

Some material also was published in the PhD thesis of Sarah Kaiser [133].

4.1 Introduction

Demonstrations of QKD with moving airborne platforms take important steps to verifying the readiness of quantum technology, and the supporting classical technology, for deployment within a satellite payload. QKD to aircraft platforms currently has only been demonstrated in down-link configurations [74, 75], where the source is located on the aircraft and the signals are sent to a receiver at a ground station. Our experiment, described in Chapters 4 to 6, demonstrates a QKD up-link to a receiver on an airplane. The apparatuses utilize coarse- and fine-pointing systems necessary to establish and maintain the optical link, quantum source and measurement components that conduct polarization-encoded QKD, and suitable post-processing algorithms to extract secure key.

Many components in the QKD receiver used here are custom-designed according to the mass, volume, power, thermal, and vacuum operating environment requirements of

systems to be used in a satellite payload—many components are already space suitable, and others have a clear path to flight. The demonstration explained here displays the technological advancements made towards the development of a space-suitable QKD receiver, and highlights the feasibility and technological readiness of an up-link QKD satellite.

4.2 Project Management

This project consisted of a large team consisting of members from the Quantum Photonics Laboratory (QPL) at the Institute for Quantum Computing/Department of Physics and Astronomy, as well as members from the National Research Council of Canada (NRC) Flight Research Laboratory (FRL). The official project began in April 2014 when QPL received the CSA Flights for the Advancement of Science and Technology (FAST) grant which had the mission of developing our payload and testing it on an airborne platform. Original studies involved the possibility of using a stratospheric balloon, and eventually evolved into using an airplane. A summary schedule of important events is shown in Table 4.1. Official collaboration with the NRC began in February 2016, and between then and September 2016 there were many teleconferences, phone calls, and visits to the NRC FRL to plan logistics for the project.

As the project manager, I was the point of contact between the two organizations as well as in charge of furthering experimental progress. Some of the duties included in managing this project were information dissemination, travel arrangements, proper report filing (both for UW and NRC), planning of experimental tests, planning of flight requirements, and many more. I was also responsible for ensuring all regulations required by the University and the NRC were met for this experiment, which included training, forms, and health and safety. Since the experiment was located about a 5 h drive from our lab, I also had to make travel and lodging arrangements for our team. The IQC team met weekly to discuss progress as well as issues with equipment, etc., from 2014–2016.

During the course of the project, I traveled to the NRC FRL three times. The first trip in April, 2016, was for one day to see and take accommodation measurements of the aircrafts offered by the NRC, to determine which one would best suit our needs. The receiver equipment was brought on this trip to attempt fitting in candidate aircrafts. The second trip was in July, 2016, for one week, again bringing all the equipment that would be mounted into the aircraft. During this week, the NRC mechanical staff measured the equipment to determine what would need to be changed/re-built in order to meet airworthiness standards. I also visited Smiths Falls–Montague Airport (CYSH) during

Event	Date
Develop QKD receiver components	2014
Received CSA FAST grant	April 2014
QKD to moving truck	Summer 2014
Visit STRATOS campaign launch site	September 2014
Fine pointing system developed	Dec 2014-Sept 2015
Stratospheric balloon concept ruled out	Spring 2015
Searching for aircraft options	Summer/Fall 2015
Full QKD with new receiver equipment in lab	Fall 2015
Establish collaboration with NRC	February 2016
Visit NRC to see aircraft options	April 2016
Outdoor testing of new QKD receiver payload at UW	Spring/Summer 2016
First established outdoor QKD link with new hardware	July 2016
Visit NRC to determine airworthiness of receiver payload	July 2016
Further outdoor testing at UW	August 2016
First successful link to 3 km site	September 6, 2016
Payload integration and ground station setup at Smiths Falls	Sept 12-16, 2016
Final testing and flights	Sept 19-22, 2016
Dismantling ground station and receiver	Sept 22, 2016
Data analysis and review	October-December 2016
Publication released (arXiv)	December 2016
Published (Quantum Science and Technology)	June 2017

Table 4.1: Time line summary of important milestones and events during the airborne project from receiving the grant to publishing the paper.

this trip to look at potential ground station locations. The final trip for two weeks in September, 2016, was for conducting the experiment itself. The first week was used to setup the ground station and to integrate the receiver payload onto the aircraft, as well as reassemble new pieces which were machined by the NRC staff. The second week is when the experiment took place.

A shortlist of possible sites at Smiths Falls–Montague Airport were selected. For any ground station location, permission would be needed from the manager of the facility to park our trailer for two weeks on their land. Our selected site was located where it would have minimal background light, but also have minimal impact on the operations of the airport. This was important as the airport is used widely for private flights from the flying club. A flyer was created and posted in the main office building of the airport with information about our experiment and contact details in case of questions.

Throughout the months of planning, I was in frequent communication with the NRC to make sure that they had all the information regarding our equipment as well as the requirements we needed to perform a successful experiment. I was also in charge of setting up the test experiments at the University on North Campus from the dome on the roof of the Research Advancement Center 1 to the truck. These tests were performed from June, 2016, to September, 2016, with all the new equipment from the QKD receiver (QKDR) project completed in the previous two years since the truck experiment in 2014. This meant organizing the team to be able to perform these tests and troubleshoot the problems that arose from the new equipment.

4.3 Feasibility and Requirements

Previous studies had indicated that an aircraft would be a better option over a stratospheric balloon [133], which meant we could move forward with preliminary tests to determine the proper equipment and scale to which we could perform the experiment. Although the aircraft would not offer the same environmental considerations that a balloon would offer, the ability to achieve angular speeds similar to that of LEO satellites was beneficial. These typically (as for QEYSSAT) can be around $0.7\,^{\circ}/\mathrm{s}$ but can be as fast as $1.2\,^{\circ}/\mathrm{s}$ (for the ISS). Table 4.2 shows the angular rates for various speeds of the aircraft and various ground distances between the aircraft and the ground station.

Table 4.3 shows the angle the telescope would be required to point down based on the distance the aircraft is from the ground station. Figure 4.1 demonstrates the allowed ground distances and altitudes for a few selected angles. The acceptable area is above the

Ground Distance[km] Aircraft Speed [knot]	3	5	7	9
90	0.88 °/s	0.53 °/s	0.38 °/s	0.29 °/s
100	0.98 °/s	0.59 °/s	0.42 °/s	0.33 °/s
110	1.08 °/s	0.65 °/s	0.46 °/s	0.36 °/s
120	1.17 °/s	0.70 °/s	0.50 °/s	0.39 °/s

Table 4.2: Angular speeds of the aircraft experienced by the ground station, based on the speed of the airplane as well as its ground distance.

Ground Distance[km] Altitude [km]	3	5	7	9
1	18°	11°	8°	6°
2	33°	21°	15°	13°
3	45°	31°	23°	18°

Table 4.3: The angle the receiver telescope would have to make below horizontal for various ground distance and altitudes. For the Bell 206, the angle has to between 30° and 45°. The Twin Otter has no restrictions down to 45°.

curves, which represent the angle which the telescope makes below horizontal. The black horizontal line is 3 km which is the maximum allowed altitude of flight by these aircraft without using oxygen masks.

After the collaboration with the NRC was established, two potential aircraft were identified for this experiment: a Bell 206 Helicopter, and a Twin Otter fixed-wing dual-propeller airplane. The first step was to determine whether our equipment would fit into the aircraft. Measurements were taken of the QKD equipment as well as the aircraft and schematic images were created to determine the fit. These placements can be seen in Figure 4.2. The main goal, as learned from the Beechcraft Bonanza fitting described further on, was to be able to get a large horizontal angular sweep to allow for flight paths other than circles.

Fitting the receiver telescope into the Bell 206 (Figure 4.2(b)/(c)) showed some restrictions in both the horizontal and vertical directions. The rear door, where the telescope points, would have to be removed. With this door removed, the telescope was restricted to pointing down between 30° and 45° below the horizon. This was concerning as it would limit minimum distance the aircraft could be to the ground station. The electronics, which were mounted in 19" rack mountable boxes, would also have to be repackaged as there was no 19" rack mounts in the helicopter.

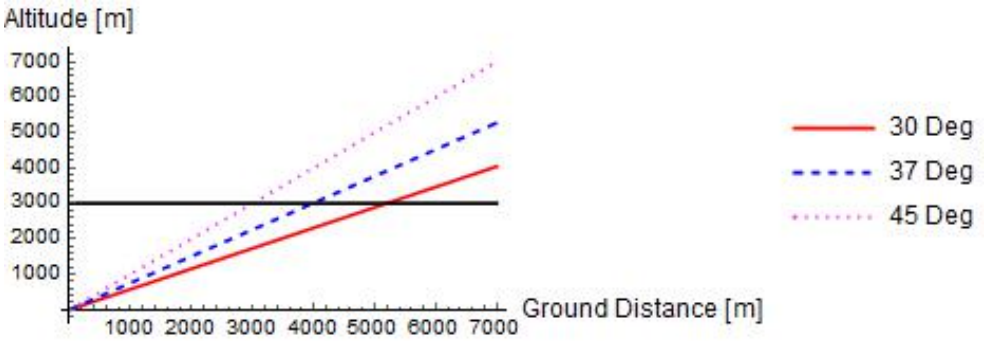


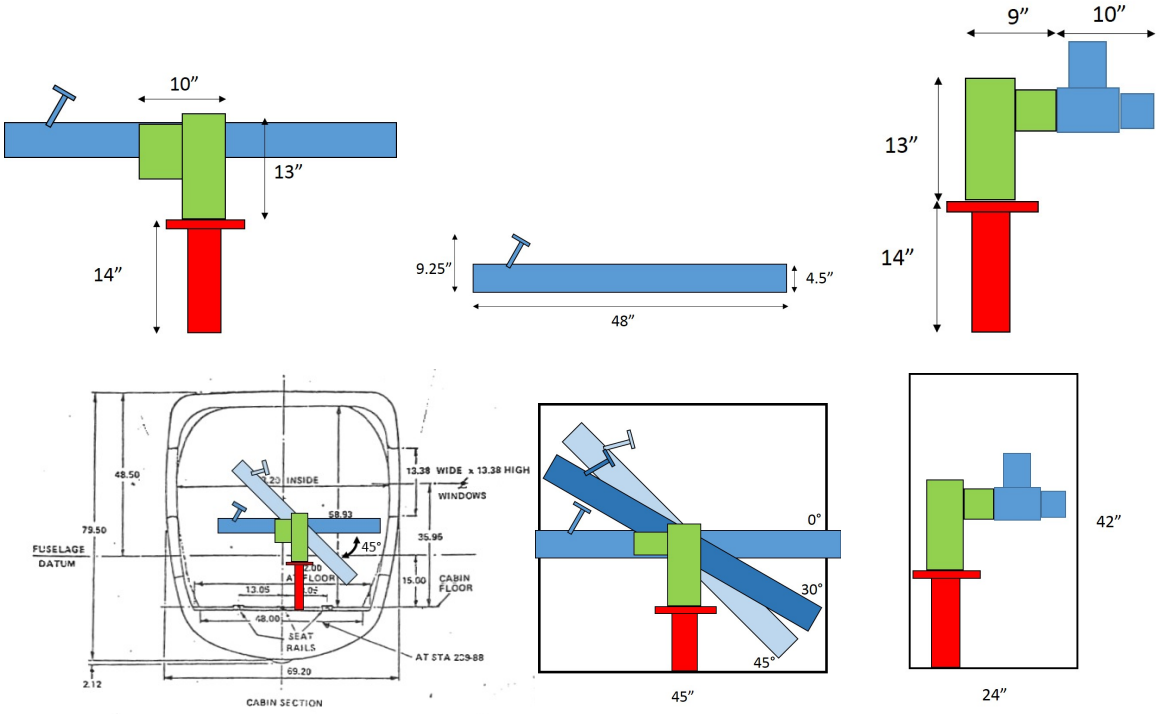
Figure 4.1: Acceptable ground distances and altitudes lie above the curves (angle of telescope below horizontal) presented in this figure. The Bell 206 has a very restrictive set of angles possible due to the width of the aircraft as well as the size of the open door, but the larger size of the Twin Otter allows the angle requirement to be relaxed which increases the distances which can be achieved.

In the Twin Otter, the restrictions on movement were much less stringent, and if the door was removed, the telescope could point down 45° and the horizontal sweep could be approximately ±40°.

A link analysis was also performed to estimate the distances and altitudes the loss budget could handle for the QKD protocol. Figure 4.3 shows the link loss as a function of ground distance and altitude. These initial calculations assumed a pointing accuracy of 87 µrad and a receiver efficiency of 25 %. The system can tolerate around 43 dB of loss (based on previous studies) which restricts the altitude and ground distance of the aircraft. If greater pointing accuracy can be achieved, the distances can be increased.

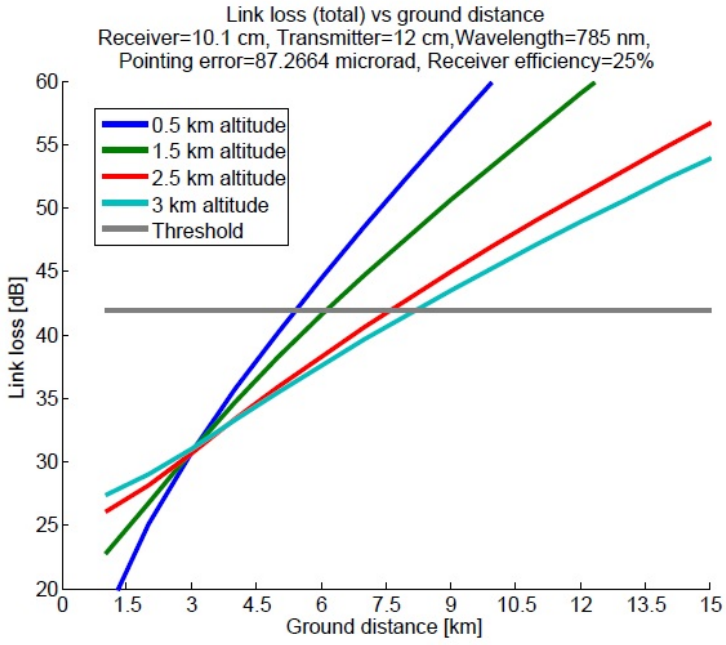
Our theoretical loss model [89] assumes a mid-latitude, rural atmospheric model in summer with the ground station located 128 m above sea level and 5 km visibility. Other model parameters include 43 % detector efficiency and receiver optical transmittance of 59.7 % (determined from the measured properties of the receiver prototype). We simulate the effect of atmospheric turbulence at our location using HV parameterization of atmospheric conditions [99, 115], with a sea-level turbulence strength of $1.7 \times 10^{-14}\,\mathrm{m}^{-2/3}$ and high-altitude wind-speed of 21 m/s. The measured pointing accuracy, aircraft altitude, and ground distance for each pass was used after the experiments to increase the accuracy of the modeling. In the model we assume diffraction-limited divergence of the transmitted QKD signal, resulting in lower bound theoretical loss estimates.

Table 4.4 shows the advantages and disadvantages of the Bell 206 Helicopter and the Twin Otter Airplane. Evaluating this, it was decided that the Twin Otter Airplane offered the best chance of success for the QKD experiments, and thus it was the aircraft chosen.

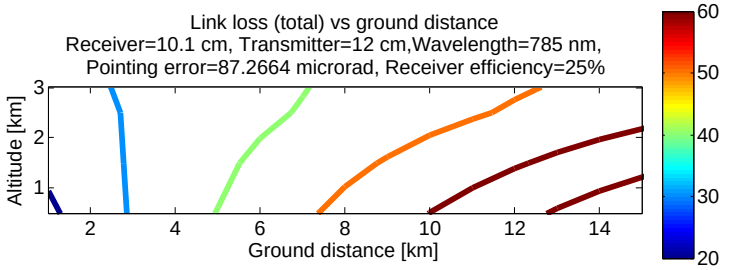


(a) (b) (c)

Figure 4.2: The top three diagrams represent the rough spatial extents of the receiver telescope along with the FLIR motor mount with pedestal. The measurements are shown for the various pieces which will need to be placed in the aircraft. (a) The receiver telescope placed over a drawing of the body of the Twin Otter airplane. The receiver has been scaled to the dimensions of the drawing. Good range of motion was seen for this option. (b) The outer box is the room which would be available in the Bell 206 helicopter as looking from the back of the aircraft. The telescope is wider than the helicopter, and would protrude outside the fuselage when at horizontal, but between 30° and 45° below horizontal it would remain inside. (c) The outer box represents the area available in the Bell 206 as viewed from the side of the aircraft. The horizontal sweep was mostly limited by the back of the telescope coming in contact with the roof.



(a)



(b)

Figure 4.3: (a) Link loss as a function of ground distance for various flight altitudes. For a 1.5 km flight this limits the ground distance to approximately 6 km. The grey bar signifies the maximum tolerable loss the system can accommodate (b) Link Loss as a function of altitude and ground distance. The operable range is to the left of the green (third) line.

	Advantages	Disadvantages
Bell 206 Helicopter	• Hovering • Slower Speeds Available • Landing/takeoff easier	• Vibration • Placement of electronics • Hardware integrity due to vibrations • No access to payload during flight • Space for only one QKD operator
Twin Otter Fixed Wing	• Low vibration • Large angular range available • Plenty of space for fitting electronics • Can switch between visible and IR lasers easily (for troubleshooting) • Space for more than one QKD operator	• Scheduling • Take off and landing are time consuming • Minimum speed

Table 4.4: Pros and Cons of the two types of aircraft offered by the NRC.

4.4 Preliminary Tests

One of the first things tested was the WiFi equipment (Ubiquiti Rocket M2 and NanoStation M) that had been used for the truck experiments. The WiFi is crucial for the pointing method as it allowed the transfer of the GPS coordinates from the transmitter and receiver to be sent to each other; since the plane's coordinates could not be predicted precisely in advance, this was necessary. This was tested both down a 10 km stretch of road as well as in an aircraft.

The airborne test of the WiFi equipment took place with the help of a private plane operator out of the Brampton Airport. The WiFi antenna was installed into a Beechcraft Bonanza airplane in the back window facing outward. A VN-300 was also placed in the aircraft as a global positioning system (GPS) receiver. Figure 4.4(b) shows the WiFi antenna mounted in the airplane.

The large WiFi antenna was held in the back of a pickup truck in the parking lot of the Brampton Airport, with an operator standing with it to turn it towards the aircraft as it flew past. The airplane took off and flew over the ground crew before circling around to perform the first link test. Each loop had the plane fly over the ground crew (no link was available at this time due to the fixed antenna pointing in the aircraft which was directly above the ground crew), which allowed them to establish a visual link with the plane. In total, the plane flew five loops around the ground station. The successful WiFi links are illustrated in Figure 4.5. Table 4.5 shows the nominal distance of the loops as well as the total established link time. Due to the arrival of a snow storm, the tests had to be cut short before a distance of 10 km could be reached.

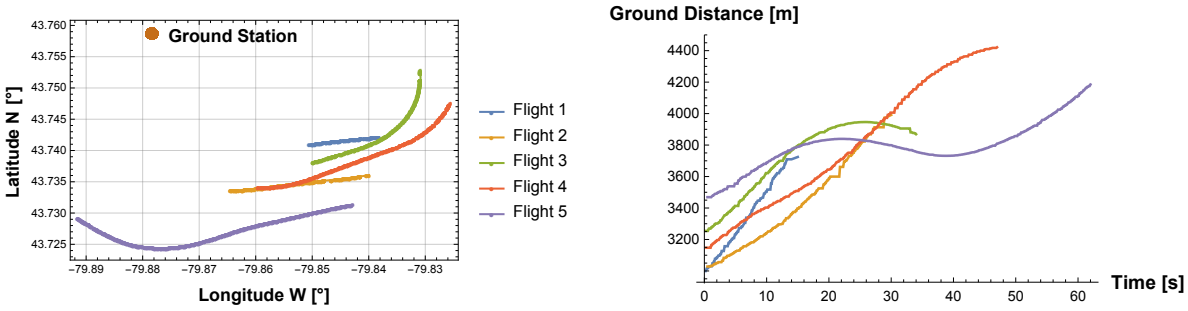
The receiver telescope and electronics were also fit into the Beechcraft Bonanza to

Flight	Average Distance [km]	Duration [s]
1	3.70	13.65
2	4.00	28.29
3	3.96	33.75
4	4.43	46.41
5	4.19	61.00

Table 4.5: Average distances between the ground projection of the airplane to the ground station and the length of time the link was maintained. The ground station WiFi antenna was actively aimed towards the airplane, but the aircraft WiFi antenna remained fixed in the airplane.

(a) (b)

Figure 4.4: (a) The Beechcraft Bonanza airplane used for testing the WiFi equipment planned to be used for the classical link during the QKD trials. (b) The WiFi antenna mounted into the rear window of the airplane.



(a) (b)

Figure 4.5: (a) The latitude and longitude of the airplane, acquired by the VN-300 and transmitted over the WiFi link to the ground station. (b) The distances measured during the WiFi link time. This distance is the distance directly below the airplane on the Earth's surface to the ground station.

Figure 4.6: The receiver telescope mounted into the Beechcraft Bonanza airplane. The telescope looks out the rear baggage compartment door, and has a small angular sweep of approximately 10° because the rear of the telescope hits the window on the other side. The front of the electronics crate can also be seen towards the left of the photo.

determine if there was enough space in this aircraft (note that this was done prior to selecting the Twin Otter). The telescope in the airplane can be seen in Figure 4.6. The angular sweep that the telescope could move through was very small (≈10°) which would not allow for a sufficient link time in a non circular flight pass. It could work if the plane flew around the ground station in a circle though.

Multiple tests took place with the truck in three locations: the parking lot in front of SAP near the Research Advancement Center (RAC) (where the ground station was located for such tests), along a road approximately 1.21 km from RAC, and a local park approximately 3.27 km away from the ground station. The locations can be seen in Figure 4.7.

The test to the parking lot in front of SAP was used as a first demonstration of the system outdoors. The equipment was loaded onto the back of the pickup truck and parked in the parking lot. The primary equipment to test at this stage was the FPU, as the device had previously only been tested in the lab. With the receiver system mounted on the truck, a link was established and photons were sent from the ground station to the receiver. The fine pointing parameters can be found in Figure 4.8.

For this test, the truck was running and a few times we shook the truck to try to misalign the pointing. The coarse pointing was not running during this time. The mean spot

Figure 4.7: The two sites for the local tests of the equipment developed for the QKD receiver. The truck drove along a road approximately 1.21 km away from the ground station and a stationary site was chosen approximately 3.27 km from the ground station. Imagery and map data ©2017 Google.

position on the QD was 0.022 µm and 0.018 µm for x and y respectively (for a description of how the device works, please refer to Chapter 3). The standard deviation in the x and y directions were 14.58 µm and 39.28 µm respectively. The shaking of the truck increased in amplitude for each of the four tests. The performance still showed counts going through the system for these deviations; there were minor drops but the counts recovered following the shaking. The noticeable decrease in beacon power was due to the truck not settling to the initial aligned position after shaking.

An issue that arose during the initial parking lot tests was the divergence of the beacons. The initial GPS acquisition software was not accurate enough to get the beacons onto the camera for the next stage of pointing, especially at closer distances. The first beacon divergences which were tested had a divergence of 5 mrad. Once these were deemed to be too small, 13 mrad divergence fibers were installed. This eliminated the problem with the initial acquisition. We also installed a bright infra-red light-emitting diode array on the receiver which had a large divergence ($> 80°$) to help with the acquisition.

The second version of the outdoor experiments involved pointing and tracking and signal collection while the truck was moving. This took place to the road which was approximately 1.21 km from the ground station. The FPU tracking results for one such run can be seen in Figure 4.9.

For this test, the truck was driving down the road at speeds up to approximately 30 km/h. The coarse pointing was running during this time. The mean spot position on

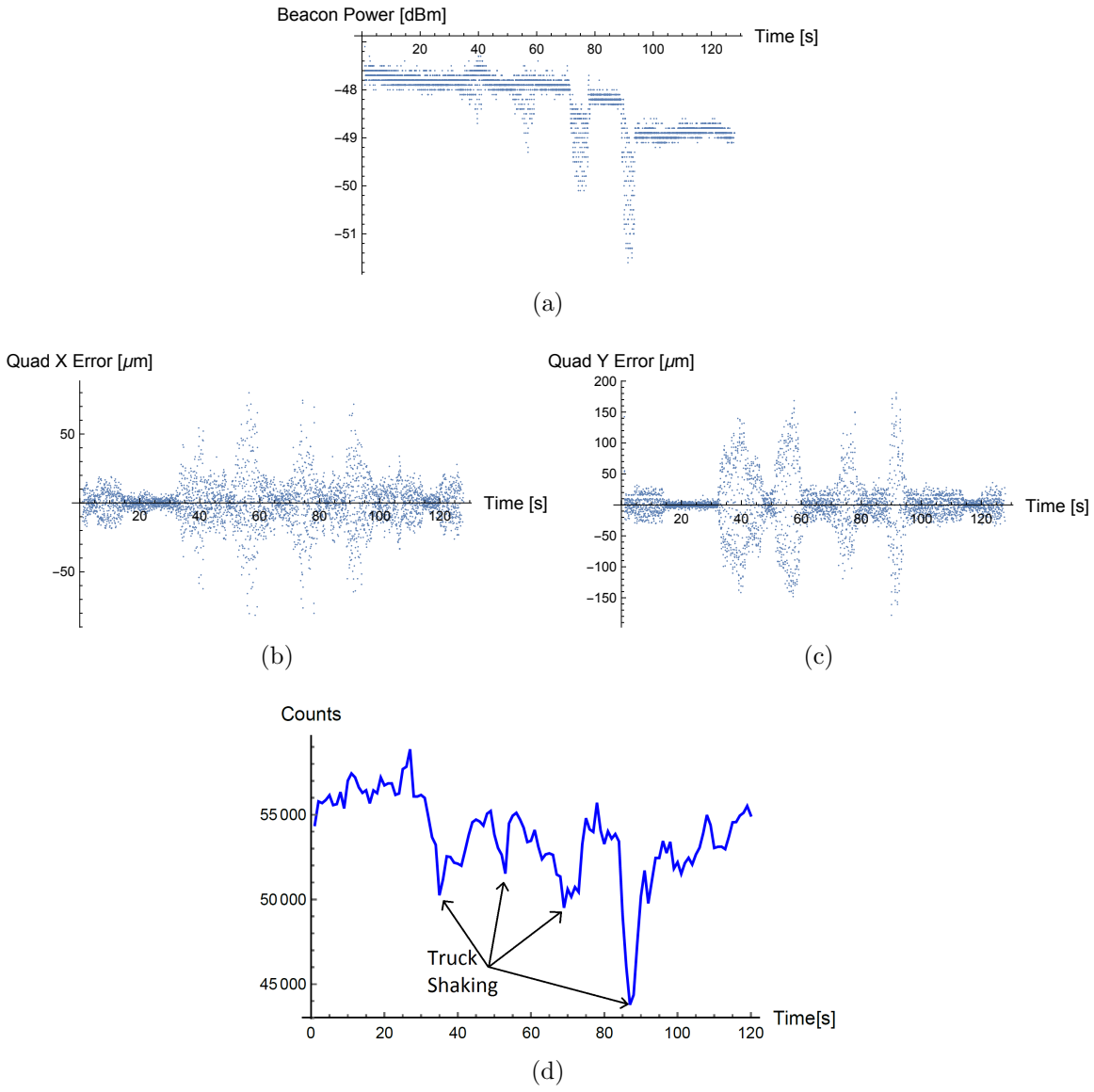


Figure 4.8: FPU performance while the truck was parked at the SAP parking lot approximately 300 m away from the ground station. The truck was running while a team member shook the truck four separate times during the run. (a) Beacon power monitored with noticeable drops during the shaking of the truck. The overall decrease is due to the truck resettling in a different location than it was when it was aligned at the beginning. (b) The x error on the QD. (c) The y error on the QD. The error in the first shake is 64.8 µm. (d) Detected single photons. There is a slight time shift between the FPU time scale and the counts time scale but four dips can bee seen corresponding with the FPU error increases.

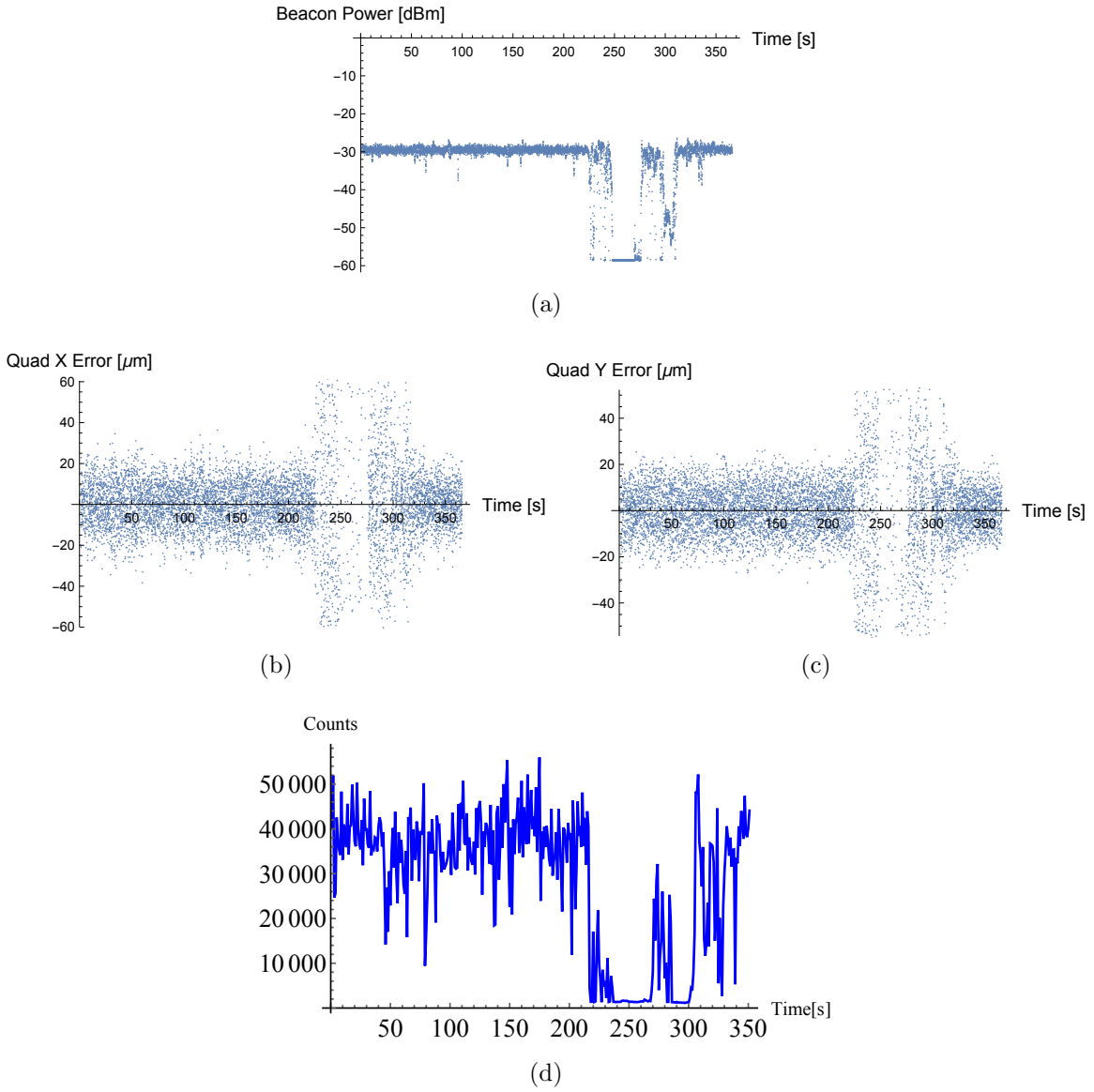


Figure 4.9: FPU performance while the truck was driving on the road approximately 1.2 km away from the ground station. The drop-out near the end was when the truck drove behind a patch of trees and the signal was briefly lost; once the truck reversed, the signal was reacquired. The truck drove up to a speed of approximately 30 km/h. (a) Beacon power monitored through the run. (b) The x error on the QD. (c) The y error on the QD. (d) Detected single photons.

the QD was $-0.045\,\mu m$ and $0.15\,\mu m$ for x and y, respectively. The standard deviation in the x and y directions were $10.72\,\mu m$ and $9.47\,\mu m$, respectively, while the tracking was running with a beacon signal. Near the end of the run, the truck went behind tree cover and the signal was partially lost. After backing up the signal was recovered. Counts were observed going through the system for these tests as well.

In order to test the initial acquisition and targeting abilities of the system at longer distances, the receiver was taken to a municipal park approximately 3 km away from the ground station. The test started by calibrating the transmitter pointing with a "mock receiver" to align the beacon and quantum signals. This mock receiver had a 3 laser beacon array with a camera attached to a small telescope. The spot from the transmitter beacons could be viewed on the camera, and the power of the quantum signal could be measured that was received through the telescope. For the first few trials, no signal was sent through the receiver. Once a realignment of the transmitter was completed, signal acquisition occurred and count rates were observed immediately. This verified the local calibration of the transmitter without using the receiver apparatus.

4.5 Flight Planning

We focused on two path types for the demonstration: arcs with (approximately) constant radius around the ground station, and straight lines past the ground station. For straight line paths, the distance to describe the pass is the minimum ground distance from the receiver to the transmitter.

In order to describe the paths to the pilots, a sequence of GPS coordinates was calculated for each flight. For the circular tracks, the start angle relative to the ground station, the angular sweep, the distance, and the ground station coordinates were used as input. The linear track calculator used the ground station location, the bearing from the ground station to the minimal distance, and the possible azimuthal sweep of the telescope in the airplane as input. The calculations for this were implemented in an Excel spreadsheet and can be found in Appendix B. The output from these sheets were waypoint coordinates in degree decimal minute format. With the assumption of local flat euclidean space, the spreadsheet was able to generate points containing latitude and longitude information. For the circular paths, approximately 10 points were generated for each path, and for the linear paths, the start and end points were generated. These coordinates were transferred to the flight software of the aircraft by the pilots.

We were allotted a total of five hours of flight time by the NRC. One systems-test

Figure 4.10: A photo out the open side door of the Twin Otter airplane, looking towards Smiths Falls–Montague Airport where the ground station was located. The telescope can be seen in the far left of the image.

day-time flight was conducted on September 19, 2017, (where the optical links were not attempted) to ensure the equipment was securely mounted in the plane, as well as to test the GPS pointing algorithm. During this flight, the pointing program was initiated and the camera image was monitored to view where the telescope was looking. Since the flight was in daylight, even with the 850 nm filter on the camera, a clear image was visible. The camera had the airfield in sight during times when the WiFi link was established. This flight lasted an hour, including take-off, transit, circling the ground station, and landing.

The NRC provided the ground station with two radio frequency (RF) radios which were able to contact the pilot, and the aircrew could communicate through the pilot any messages about change in flight plans, if necessary. This was the method used to convey when the system was functional during the flights.

Two night-time flights were conducted for the actual experiment, each of two hours duration and consisting of several passes of varying trajectories. These flights took place on September 20 and 21, 2017. Part of the experimental risk mitigation strategy was to develop a decision tree such that, based on the observed performance of each pass, we could immediately select an appropriate course of action (e.g., to perform troubleshooting, collect data under different conditions or land). On the airplane, a fiber-coupled green laser was attached to the beacon coupler system so that visible light could be directed towards the ground station in case there was a problem with the pointing. At the ground station fibers could easily be exchanged to allow visible light to be sent towards the airplane.

Over the two nights we planned a total of 13 passes, depending on success or failure,

First Night	Second Night
Failure Tree:	5 km Arc
5 km Arc (Fast)	5 km Line
5 km Arc (Slow)	3 km Line
7 km Arc (Slow)	3 km Arc
Success Tree:	7 km Line
5 km Arc	10 km Line
5 km Line	
3 km Line	
7 km Line	
10 km Line	

Table 4.6: Flight distances and types planned for the two nights. The second night flights were planned after the first night was completed.

with nominal distances of 3 km, 5 km, 7 km, and 10 km, in both line and arc configurations, at an altitude of ≈1.6 km above sea level. The distance quoted for the line configuration is the distance of where the airplane is closest to the ground station as it flies past. Table 4.6 shows the planned patterns and nominal distances for the 13 passes. The passes for the second night were planned after the first night based on the success/failure of the first night.

Prior to each flight, the QKD team and the pilots would meet to discuss the flight details and work out any issues that either party may have. This allowed the pilots to understand the purpose of each test and allowed the QKD team to know what was possible based on the weather that night.

All the flights were conducted at approximately 1.5 km altitude after 10:00 pm EDT. The QKD operator on the aircraft would send a message to the ground station crew just prior to take-off, signaling approximately 30 minutes until arrival of the airplane at the site. Once the plane arrived on site, it would first pass by the ground station and loop around into the desired flight path. The QKD signal exchange always took place with the plane flying south of the ground station, to not interfere with Ottawa International Airport. A Notice to Airmen (NOTAM) was published in advance so other pilots and crews would know that there was the potential for laser emission in the area. The NOTAM prepared by the NRC team was:

"CYSH RED LASER LGT FOR OPTICAL ALIGNMENT BTWN A GROUND STATION AT CYSH AND RSRCH07 TWIN OTTER AIRCRAFT WITHIN 16 NM OF CYSH

AT 10,000 FT MSL AND BELOW. LASER BEAMS PROJECTING BETWEEN THE GROUND STATION AND AIRCRAFT WITHIN AN ARC BETWEEN 120 DEG RADIAL TO 260 DEG RADIAL FROM CYSH AT ANGLES UP TO 45 DEG. LASER LGT BEAMS MAY BE INJURIOUS TO PILOTS/AIRCREW AND PASSENTERS EYES WITHIN 22 FT SLANT RANGE OF THE LASER LGT SOURCES. FLASHBLINDNESS AND COCKPIT ILLUMINATION MAY OCCUR BEYOND THESE DIST. 160918 TIL 160924 BETWEEN 02000600UTC."

The moon was near full phase during the planned flight time, which was a potential concern for increasing background light during the experiment.

4.6 Discussion

The major goals of demonstrating the equipment on an airborne platform and of achieving angular rates similar to that of a LEO satellite were most feasibly attained through the use of the NRC Twin Otter Research Aircraft. This platform provided us the flexibility of large angular sweeps of the telescope within the cabin as well as speeds and distances necessary to achieve the goals. The airplane also allowed us more flexibility in path distances due to the removal of the vertical pointing restrictions imposed by the Bell 206 helicopter option.

The link analysis provided a baseline for the paths which could be attempted, although many of the assumptions in the model were of a worst case scenario. Therefore, the model predicted the maximum we could expect from the worst case. The biggest assumption used in this analysis was the pointing accuracy of the transmitter. Since we were unable to test this previously, this assumption influenced many of our choices.

By testing the WiFi equipment in flight and concluding successful operation, we were able to use our time to work on the QKD equipment and its integration onto the various platforms. This was especially important for moving the receiver to the airplane as many aspects required focused development.

The tests with the truck performed locally were extremely beneficial for troubleshooting problems that would not be experienced in the lab. One of these issues, it was discovered, was dew. In order to combat this problem, "dewbusters" were acquired and wrapped around the telescopes to prevent the dew from forming by heating the enclosures. This was especially a problem at the transmitter, but the receiver would be located in the airplane and would have a roof directly over top, preventing the formation of dew.

Another issue which was resolved through these local tests was the divergence of the beacons. This was increased so the initial GPS acquisition could bring the telescopes in

range of the beacons. The problem with this is that as the divergence increases, the total power per unit area at longer distances is less, restricting the distance we are able to achieve. Since the link analysis predicts longer distances not to be possible anyway, this was not deemed a concern at the time.

The flight planning was a new regime for us and, thanks to the help of the pilots of the aircraft, we were able to implement a calculation to send them what they needed. This calculation allowed us to generate way-points which would guide the pilots as they flew the plane from their flight computers.

As the receiver equipment was often in Ottawa for measurements, local tests frequently had to be halted or postponed. This was worrisome especially when the first successful truck links were established near the end of July, approximately a week before the equipment was to be dismantled and taken to the NRC.

After the week in July where the equipment was away, further tests needed to be completed for the pointing and acquisition. The equipment was assembled once again, and further tests were conducted. The last of these tests, done the week before the flight campaign was to begin, tested the link over approximately 3 km verifying further distances than just 1 km.

Chapter 5

Experimental Airborne Tests of Quantum Key Distribution

Notes

Parts of this chapter are adapted or used from material published on June 6, 2017 as [156]:

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

5.1 Experimental Setup

The apparatuses for the airborne experiment consist of a QKD source and transmitter, located at a ground station near the airstrip of Smiths Falls–Montague Airport, and a QKD receiver, located on a Twin Otter research aircraft from the NRC. Optical links were only attempted at night, to limit optical noise.

The ground station location (North 45° 45.7066 minutes, West 75° 56.6256 minutes, 127 m altitude) was chosen for multiple reasons . In discussion with the NRC, it was determined that they had contacts with the Smiths Falls Flying Club, and we also had a colleague with a hangar at the airport who offered space for storage of our equipment. The runway is also typically fairly quiet at night, allowing us to conduct laser links with minimal disruptions to the operations of the airfield.

The Twin Otter research aircraft was located at Ottawa International Airport, which was only a 10 min flight from CYSH. The CYSH airfield also had little background light

Figure 5.1: Ground station located at Smiths Falls–Montague airport, showing (left-to-right) the calibration telescope, WiFi antenna, the transmitter assembly, and the trailer where the source is located. The tent in the background is used to cover the transmitter between experiments so it does not have to be dismantled between trials.

which would allow for low noise in the signal detections. The runway lights are usually off and can be operated by pilots via radio transmission and remain on for half an hour once initiated and then turn off again. If necessary, the aircraft would also be able to land on the CYSH airstrip for troubleshooting on the ground.

The QKD source optics and electronics were located inside of a trailer to maintain thermal and humidity stability. The transmitter pointing motors, polarization compensation and characterization optics, and telescope were located just outside the trailer, with cabling running through a window. Once the transmitter tripod, motors and telescope apparatus was assembled outside the trailer, a tent was setup over top that covered the assembly when the experiment was not running. This was done so it did not have to be dismantled after each flight which could cause misalignment. Equipped with an electric generator, the ground station is relocatable and self-sufficient. The WiFi antenna was also located outside the trailer and was moved manually to track the airplane. Figure 5.1 shows a photo of the optical ground station.

The QKD receiver was mounted inside of a Twin Otter Research Airplane from the NRC. This plane was designed and flown for research purposes and has been involved in many other experiments. The staff at the NRC have the technical expertise to implement experiments on board aircraft platforms and assisted us in deploying our equipment on board. The QKD signal link between the ground station and the receiver on the airplane

was established using tracking with two-axis motors, guided by beacon lasers (at 850 nm) and a camera, on both the transmitter and the receiver. There the QKD signal polarizations and times-of-arrival were recorded for later correlation and processing to complete the QKD protocol and extract secure key.

5.1.1 Source and Transmitter

The QKD source is an improved version of a previous-generation apparatus [157], which implements BB84 with signal (probability of 80 % per pulse), decoy (probability of 14 % per pulse), and vacuum (probability of 6 % per pulse) states at 400 MHz. Weak coherent pulses at 785 nm wavelength are generated by sum frequency generation [158] with a narrow-band 1590 nm continuous-wave (CW) laser (L1) and a 1550 nm triggered-pulsing laser (L2) in a periodically poled magnesium oxide (PPMgO) waveguide (see Figure 5.2). Signal and decoy intensities are manipulated using a fast electro-optical intensity modulator (IM) calibrated to emit $\mu \approx 0.5$ and $\nu \approx 0.1$ mean photon number, respectively, at the entrance of the transmitter telescope. The vacuum state is made by suppressing the laser trigger.

Each of the four BB84 polarizations (H, V, D, and A) are created using two electro-optical phase modulators (PMs), each of them in one arm of a balanced Mach-Zehnder polarization interferometer. With a D input, the PMs can reach any state D, R, A, and L. A subsequent unitary rotation takes these to D, H, A, and V, respectively. The intensity and polarization states are generated according to a randomized sequence that repeats every 1000 pulses. Although this is insecure, it is sufficient for the demonstration and later a QRNG could be used to create this sequence.

Pulse intensities are measured locally through the weak output of an optical fiber splitter (90:10) connected to a Si-APD. The majority of the pulse power is guided from the source to the transmitter through single-mode optical fiber. The beam passes through a 785 nm band-pass (3 nm bandwidth) filter (to impede Trojan-horse attacks [159]) and then a 75:25 beam splitter. The reflected 25 % of pulses undergo characterization, while the remaining 75 % of pulses pass through three wave plates (WPs) (a sequence of quarter-, half-, and quarter-wave-plate) in motorized rotation stages that apply a compensation, as measured by the characterization system, for any rotation caused by the single-mode fiber, and are finally transmitted through a 12 cm diameter Sky-Watcher BK 1206AZ3 refractive telescope.

The polarization characterization system consists of two beam paths, where each path passes through a port of a rotating chopper wheel (the position of the wheel is recorded for the analysis) that contains linear polarizers which are each calibrated to project onto the

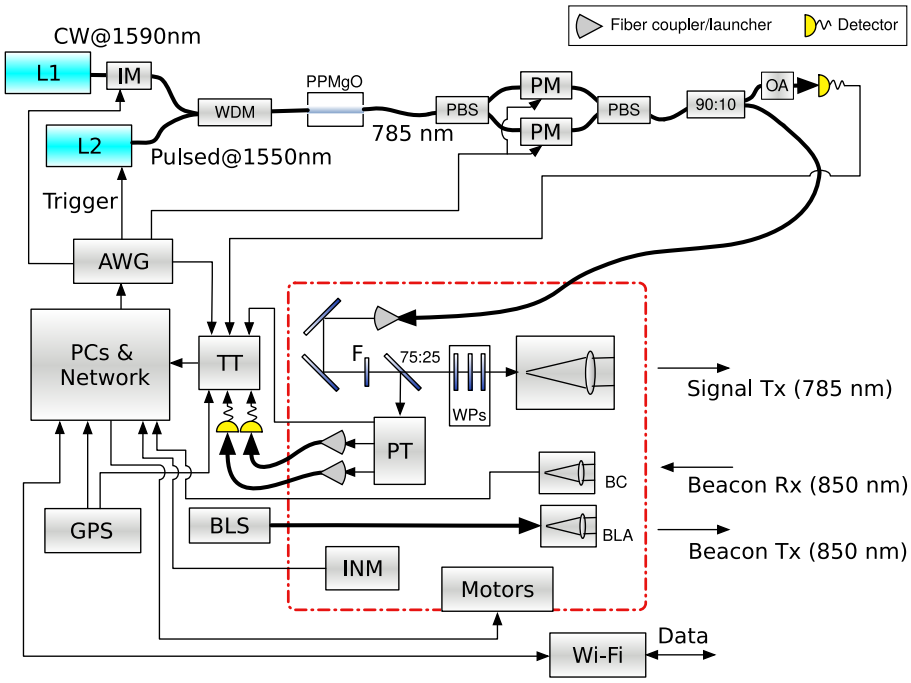


Figure 5.2: Schematic diagram of the quantum source and transmitter apparatus. Arbitrary waveform generator (AWG); wavelength division multiplexer (WDM); polarizing beam splitter (PBS); optical attenuator (OA); band-pass filter (F); polarization tomography (PT); time-tagger (TT). Other acronyms and details given in the text. The red border indicates components that are mounted on the motors.

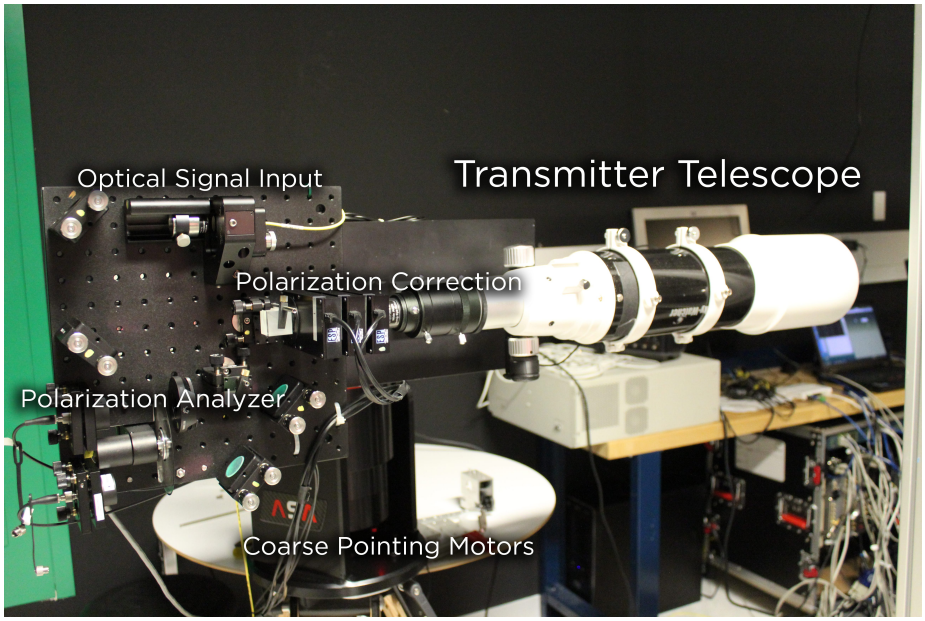


Figure 5.3: Photo of the transmitter setup in the lab. The optical signal is led from the source to a fiber launcher located at the top of the breadboard. The signal is guided by mirrors towards a 75:25 beam splitter where the 25 % arm is separated into two paths, with one passing through the rotating wheel that has slots with polarizers at various angles and collected for detection. The other arm passes through a quarter-wave-plate and then through the spinning wheel before being collected for detection. The 75 % arm passes through three wave-plates which compensate for any polarization drift caused by the transmission through the fiber from the source to the transmitter. The signal is finally transmitted toward the receiver through the transmitter telescope.

H, V, D, or A state. One of the two beam paths contains a quarter-wave plate just prior to the chopper wheel, which creates projections onto a tomographically complete set of three polarization bases: HV+, DA×, and RL○. The photons are then coupled into multi-mode fiber and measured with Si-APDs. The polarization compensation system can be seen in Figure 5.3.

The telescope and transmitter are also each wrapped with a heat strip with variable heat control to prevent the formation of dew. Dew on the optics causes high amounts of loss and can lead to experimental failure. This was frequently monitored throughout the experiment.

Many devices were connected by a local Ethernet network. This included devices at the transmitter, and devices at the receiver and could be linked with an Ethernet cable for local testing or WiFi for distance testing. Figure 5.4 shows the map of the equipment on

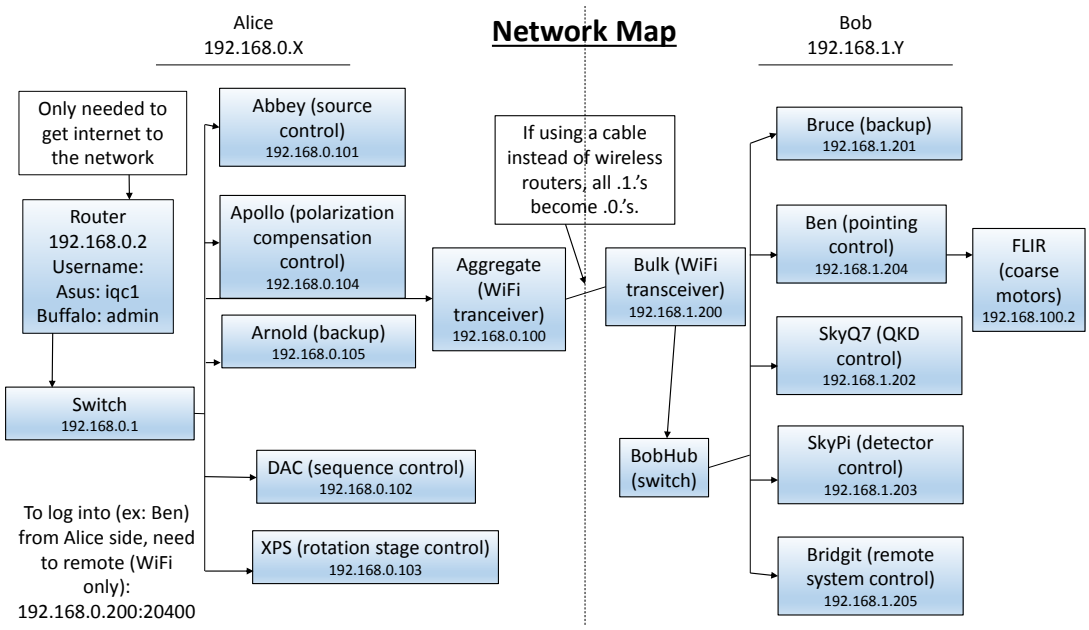
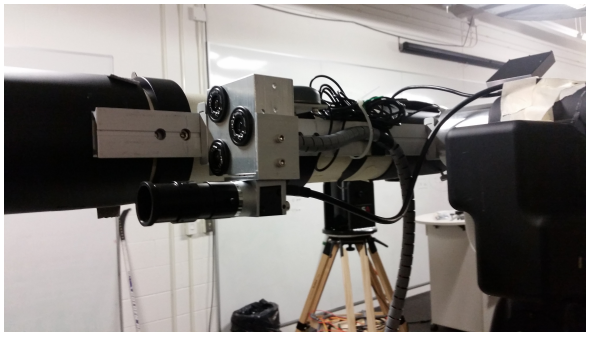


Figure 5.4: Map of the network locations for all of the equipment on both the transmitter and the receiver sides. The iqc1 router was only used when the network required internet access for updating. When the two sides were connected with an Ethernet cable Aggregate and Bulk were not used. The CDPU was named SkyQ7 and can be seen on the receiver side (Bob).

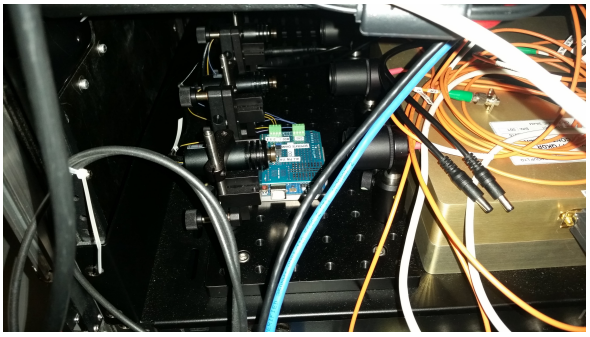
the network.

The transmitter and receiver each have a beacon laser assembly (BLA) consisting of three fiber launchers with fixed divergence angles of 0.74° and individual tip/tilt adjustment (see Figure 5.5(a)). These are mounted on each telescope and fed strong (≈40 mW) 850 nm laser light from fiber-coupled beacon laser source (BLS) arrays located away from the telescopes (see Figure 5.5(b)). A beacon camera (BC)—a 50 frame-per-second, 2 mega-pixel imaging camera with an 850 nm band-pass filter (10 nm bandwidth)—is also mounted to each telescope.

Each telescope is attached to a commercial two-axis motor system (transmitter: ASA DDM85 Standard, receiver: FLIR PTU-D300E), providing first-stage *coarse* pointing. When light at the beacon wavelength is visible as a bright spot on the camera image, the custom pointing software (running on Ben and Alice PCs at each site) controls the angular speeds of the motors to minimize the deviation of the spot's position from a calibrated reference position. The pointing software operates as a state machine, and also includes a *coasting* state to handle short drop-outs of the beacon signal, and *acquiring* and *searching* states to support the initial acquisition of the beacon. The searching state will



(a)



(b)

Figure 5.5: (a) The BLA displaying the three fiber launchers, each with separate tip/tilt control. The camera is located on the bottom of the assembly in this image but was moved to the top for the airplane experiment to match that of the transmitter. (b) The BLS where the three 850 nm beacon lasers were coupled into fibers.

cause the telescope to make an increasing radius spiral pattern to attempt to search for the opposite station.

5.1.2 Receiver

At the receiver, the signal is collected by a Tele Vue NP101is refractive telescope with a 10.1 cm aperture, and coupled into a sequence of custom components developed under contract with the Canadian Space Agency [134]. First of these is the FPU described in Chapter 3.

The FPU guides the light through a 50 µm pinhole, acting as a spatial-mode filter [160]. It then passes into a custom IOA developed with INO, containing a passive-basis-choice polarization analysis module with a 50:50 beam splitter and polarizing beam splitters [133]. The IOA produces four beams coupled into multi-mode fibers, corresponding to the four BB84 measurement states (H, V, D, and A). A metal guard was mounted across the back of the IOA to prevent any pressure from being applied to the fibers coming out of the IOA.

The four IOA output fibers, which were wrapped in black cloth to prevent excess light from entering, are guided to a detector module (DM) containing four Excelitas Technologies SLiK Si-APD detectors operating in Geiger mode with passive quenching [133] and cooled to −20 °C. They have a detection efficiency of ≈45 %, biased 28 V above breakdown.

The detectors trigger low-voltage differential signaling pulses which are measured at a control and data processing unit (CDPU) based on Xiphos Systems Corporation's Q7

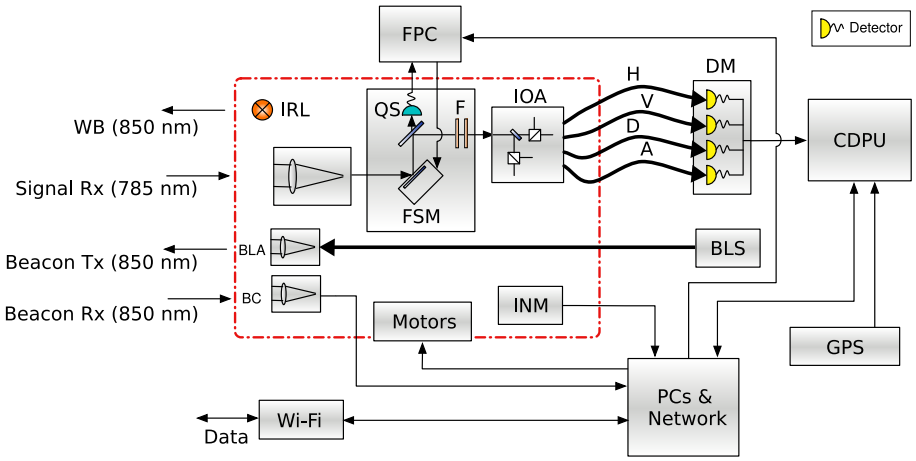
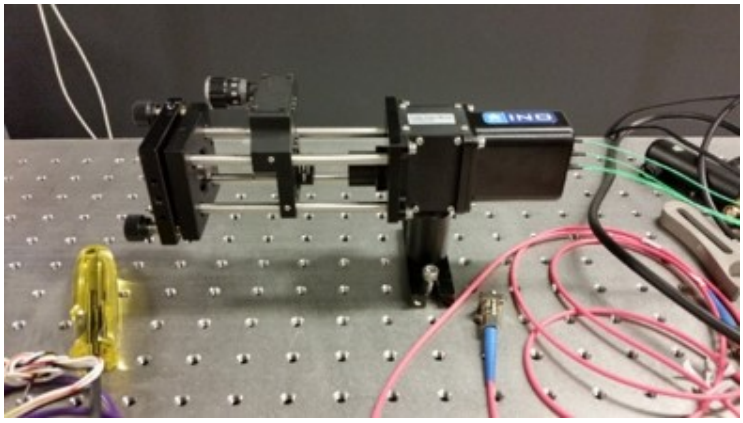


Figure 5.6: Schematic diagram of the receiver apparatus. wide-field beacon (WB) (produced by the IRL). Other acronyms and details given in the text. The red border indicates components that are mounted on the motors.

processor card, which has space heritage as it was recently flown on GHGSat [161], with a custom daughterboard. An FPGA embedded in the CDPU is programmed to implement time-tagging of detection pulses with a resolution of 78 ps, while data storage, communication, and processing software running in the Linux operating system implement the receiver-side QKD protocol. A schematic of the system can be seen in Figure 5.6 and the IOA, DM, and CDPU can be seen in Figure 5.7.

The DM and CDPU were mounted in a custom 19" rack box with four fiber couplers, two Ethernet ports, two serial ports and two BNC connection ports to give access to the devices. The four fiber couplers connect directly to the four single photon detectors. The serial ports are to allow input of a GPS signal into the CDPU and the BNC connections are for a pulse per second (PPS) input from a GPS unit to the CDPU as well. The Ethernet ports allow an external computer to connect to the CDPU and control the programs as well as the detectors via a Raspberry Pi unit.

Two 19" rack shelves were used to hold the FPU controller, the beacon laser assembly, the coarse pointing control computer, the network switch, the GPS unit, and a green alignment laser. The coarse pointing control computer was a solid state computer (to avoid risks from vibrations) which was used to run the pointing software (described below). The network switch connects all of the Ethernet accessible components together, so everything could be accessed from a single computer. The GPS unit is used to provide information to the QKD software. The Twin Otter has a permanently mounted GPS antenna and a splitter was used to route a signal from this antenna to our GPS box. The green alignment



(a)

(b)

(c)

Figure 5.7: (a) The IOA mounted with a focusing lens in a cage mount for testing. The light enters the left side of the unit through the pinhole. The main portion of the black casing contains the passive basis choice analyzer. The four fiber outputs can be seen to the right of the device. (b) The DM seen with the four modules running vertically. The IOA output fibers connect to the fiber couplers at the left. (c) The CDPU where the signals from the detectors are timestamped and the QKD software is executed.

laser was installed in case a visible signal was required to assist in alignment during the trials.

Two custom power supply units were built to supply power to the coarse pointing motors, the FPU, the WiFi antenna, the CDPU and detectors, the control computer, the beacon lasers, the network switch, the infra-red light-emitting diode array (IRL), and a green alignment laser. The larger of the two power supplies was designed to run off either 110 V AC power or unregulated 28 V DC power. The power supply can switch seamlessly between the power supplies which means the system can be powered from a battery until the plane power is turned on and supplied to the device. This allowed us to have the system on and settling before the engines for the plane were started. A large, custom lithium ion battery was used to power the equipment and could last for approximately 8 h while the system was running.

The receiver telescope was mounted facing out the cabin door on the port side of the aircraft, and flown with the door removed (Figure 5.8). A bright IRL was mounted also facing out the door, as well as the WiFi antenna. The electronics and computers were located six feet forward in the aircraft cabin, and optical fibers and cables conducted signals between the electronics and the receiver telescope pointing equipment (see Figure 5.9). A second computer was located near the front of the passenger cabin and connected via Ethernet to the local network, which allowed two operators to control the receiver components. The laptop on top of the electronics setup was used to access the computer controlling the pointing as well as the CDPU and DM.

All of the receiver equipment had to undergo airworthiness testing prior to flight, which involved analyzing all of the components and how they are mounted. The NRC conducted a stress analysis to ensure the equipment could withstand a 9 g hard-landing scenario. The main component that had to change from the original receiver setup (used in tests with the truck around the University of Waterloo Campus) was the mounting between the receiver telescope and the FLIR motor mount. The original system involved friction mounts clamping on a dovetail bar. Because of the vibration environment and the open door in the airplane, this had to be changed to a fixed mount which was done by the NRC mechanical team. A tether was also added to strap the telescope to the aluminum plate where the coarse motor system was mounted, but was sufficiently long to not inhibit movement of the telescope. All screws required lock-tight or lock-washers and the components attached to the 19” trays required Ty-Rap cable ties as well as Velcro.

An Electromagnetic Interference / Electromagnetic Compatibility ground test was also performed to verify the QKD electronics did not interfere with the cockpit avionics, and vice-versa. The NRC reported that no anomalous behavior was observed during this test

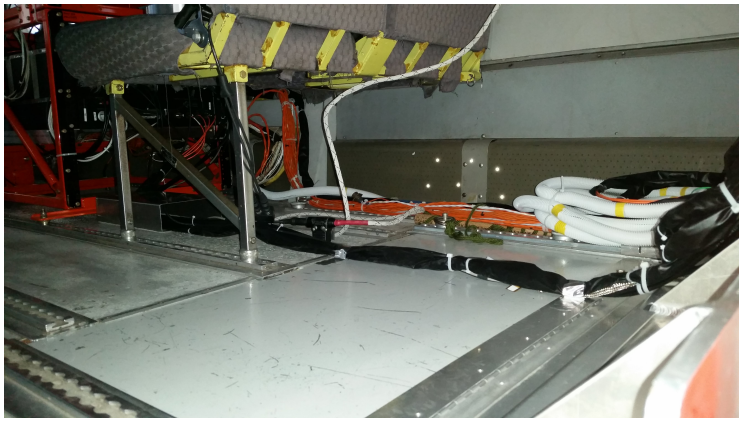
Figure 5.8: Receiver apparatus facing out the port-side door of the NRC Twin Otter research aircraft, showing (clockwise) the telescope, beacon assembly, motor mount, IRL, WiFi antenna, and fine pointing controller (FPC) (behind).

and the QKD equipment also showed no signs of disturbance.

The receiver telescope was mounted on a pre-existing bracket above the belly port in the Twin Otter aircraft. The mounting was designed such that when the telescope was pointing horizontally out the door, the edge of the telescope was flush with the body of the plane. This was chosen so the telescope never went beyond the body of the plane, thereby shielding it from direct wind exposure.

The electronics rack was assembled outside of the aircraft, and once finished was lifted inside and mounted to the floor in front of the two rear crew seats. The bracket for the receiver telescope was first placed in the aircraft, and then the coarse pointing motors and receiver were mounted onto the bracket. Cables and fibers were then fixed to the floor between the receiver and the electronics. There were seven fibers (three beacon and four signal fibers), the WiFi Ethernet and power cables, the coarse motor power and control cable, the FPU power cable and a USB cable, and the IRL power cable, running between the two locations. The controller box for the FPU was mounted on an aluminum plate beside the coarse pointing motors, as the cables connecting the controller unit to the QD and tip-tilt mirror were too short to reach the electronics crate while allowing full movement of the telescope. Thus, the only cables for the FPU that had to run to the electronics rack were a USB and a power cable.

(a)



(b)

Figure 5.9: (a) Electronics rack mounted in the aircraft. The QKD operator sat in the seat directly in front of the electronics crate and had access to all the power switches as well as a laptop to control the equipment. (b) Cables tied to the floor running from the receiver to the electronics rack. The optical fibers were covered with black cloth to prevent extra light from leaking in.

5.1.3 Acquisition and Calibration

To achieve initial acquisition, we utilize inertial navigation modules (INMs), containing GPS receivers and attitude sensors (VN-300), mounted to the telescopes. Each site transmits their GPS location to the other site via the classical WiFi link, and then calculates the other site's orientation relative to its own based on its local attitude data. During initial testing, the INMs exhibited an attitude uncertainty of about $\pm 2.5°$—significantly larger than the $0.74°$ divergence of the beacon lasers. To mitigate this, we turn on the bright IRL at the receiver, allowing the transmitter to find, and point towards, the receiver. Once the receiver sees the transmitter's beacon spot in its camera image and has moved to position, the IRL is switched off by the QKD operator on the airplane, and two-way beacon tracking continues for the remainder of the pass.

The antennae for the INM on the receiver are located inside the airplane and therefore do not have a clear view of the sky. It was initially a concern that it would not be able to get sufficiently accurate GPS results because of the metal frame of the airplane, so the pointing software was programmed with the capability to utilize the inertial and GPS data streamed from the aircraft inertial navigation system. This was put in place as a backup if the VN-300 could not get signal.

A necessary practical feature of the transmitter and receiver apparatuses is that they can be independently calibrated, as they would not be co-located prior to establishing a link (much like for a satellite mission). To make sure the beacons and quantum signal were collinear, we first inject alignment laser power into each telescope, and point the telescope towards a separate larger-diameter ($\approx$20 cm) telescope, located $\approx$20 m away, equipped with a camera imaging the far field. A diagram of this apparatus can be found in Figure 5.10. We then observe the position of the beacon beams on the camera image, and adjust the tip and tilt of each beacon fiber launcher to center its output over the signal spot. To calibrate the reference position of the beacon camera at the transmitter and the collimation of the transmitted quantum beam, we optimize the power received (using the alignment laser injected into the transmitter telescope) by the mock receiver located at a sufficient distance $\approx$850 m down the runway. The receiver beacon camera, which has greater tolerance due to the receiver's FPU, is calibrated using a corner cube located $\approx$50 m away in the NRC hangar. The filters in the FPU were removed to send through visible light from the receiver telescope for the calibration. These alignments were done prior to each flight and allowed link acquisition to begin immediately upon the arrival of the airplane in the vicinity of the ground station.

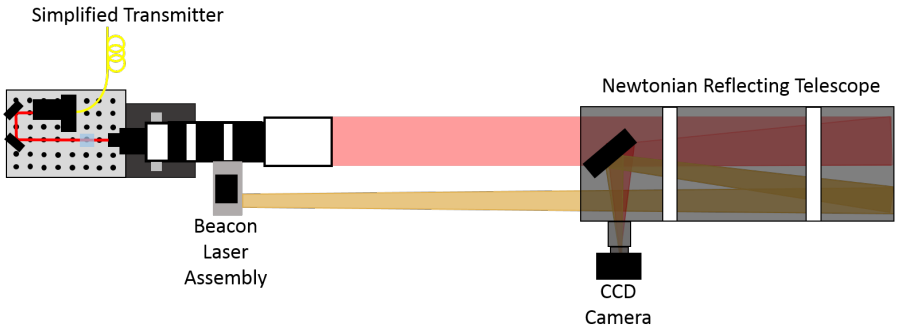


Figure 5.10: A simplified sketch of the transmitter on the left (removed the polarization compensation and characterization systems) transmits a signal through the telescope as well as through one beacon fiber launcher at a time. The beams enter a larger Newtonian reflecting telescope, focused on the far field, and are focused to a spot on a CCD camera. The beacon fiber launcher is adjusted so the beam appears in the center of the beam transmitted from the telescope. This is then repeated for the remaining two beacon fiber launchers.

5.2 Experiment

Prior to the flights, the crew members were fitted with safety harnesses which attached to the floor of the airplane. Each harness allowed enough movement room for the QKD operator to access the receiver equipment, but not exit the door. While seated, they had full access to the electronics panels and could power on or off any piece of equipment. The laptop computer was connected to all of the electronics, for control and monitoring performance.

During the first three passes on the first night we did not achieve an optical link, and were following the failure tree from the planned flights. As determined during development of the failure tree in Section 4.5, we landed at this point and were able to pinpoint the problem as being a misalignment between the beacons and the quantum signal at the transmitter (ultimately we discovered that this was due to the lens assembly at the transmitter's beacon camera being loose). We injected visible light into the telescope and, when viewing the beacons on the camera at the airplane, the quantum channel signal was clearly visible on the side of the aircraft. This was quickly re-aligned by hand at the transmitter while members at the aircraft side gave verbal instructions through cell phones, and the airplane was back in the air within 20 minutes of landing (the green laser in the receiver payload was also used to ensure the receiver was properly aligned and no issues were detected). The next pass of the aircraft around the ground station was successful in achieving a quantum

First Night	Second Night
5 km Arc	5 km Arc
5 km Arc	3 km Line
7 km Arc	3 km Line
5 km Arc	3 km Arc
5 km Line	7 km Line
3 km Line	7 km Arc
7 km Line	10 km Arc

Table 5.1: Flight distances and types for the 14 passes over the two night flights.

link and we proceeded to follow the success tree. The passes which were flown can be found in Table 5.1.

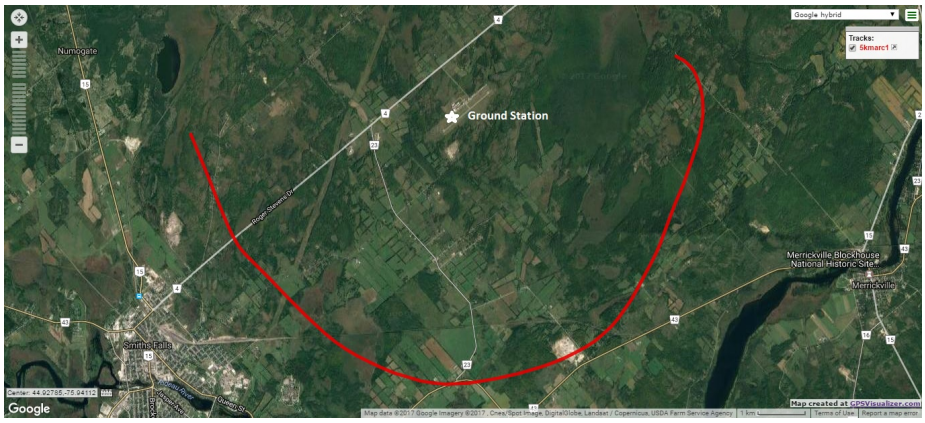
On the ground, the crew monitored the source QBER and polarization states as determined by the polarization compensation system. At one point, a wave-plate stopped rotating but was immediately fixed and did not interfere with a flight pass. The pointing software was also monitored to stop the motors after each pass and to stop any spurious tracking or motions if other sources were visible. The motors were manually set back to the south west quadrant of the sky after each pass to be ready for the next pass.

On the airplane, the detectors were turned on and cooled to $-20\,^{\circ}\mathrm{C}$ prior to takeoff. Three programs were required to be running on the computers: the coarse pointing, the fine pointing, and the data acquisition and monitoring program. The coarse pointing program was monitored each pass to ensure that the beam spot was visible and that a tracking lock had been achieved. At the beginning of each pass, the fine pointing system was started, but would only track once a beacon lock was initiated. The count collection program displayed, once per second, the counts entering the detectors.

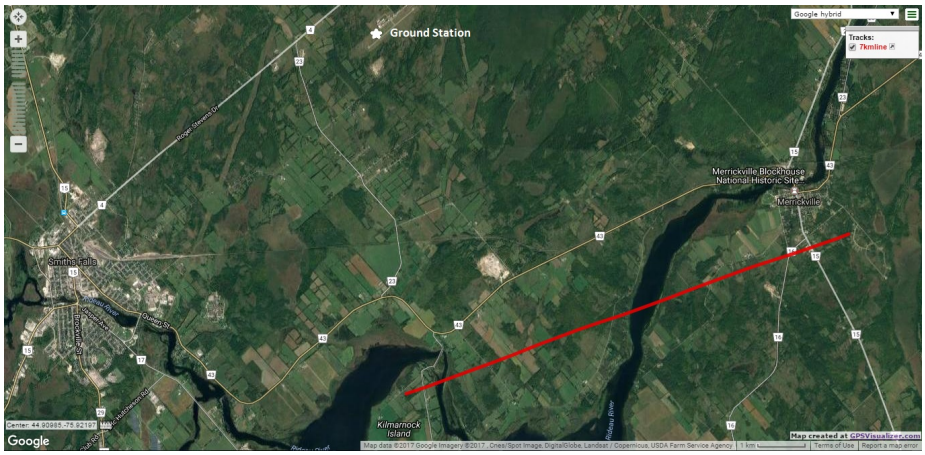
During the fourth pass on the first night (after the transmitter alignment was corrected) the real photon detection counts were clearly visible in the monitoring program, and the QKD operator signaled to the pilot that photons had been received. The pilot then radioed the ground station and informed them of the success.

The actual flight paths, where a quantum signal was exchanged, can be found in Figures 5.11 through 5.13. The 5 km arc from the second night is not shown as optimization tests were being conducted during this pass, although it is similar to the first night 5 km arc.

The WiFi transceiver at the ground station was rotated manually with visual tracking of the airplane. Because the airfield was quiet during the nights and the sky was clear, it was not difficult to view the plane from the ground station. The aircraft lights were left on



(a) 5 km Arc 1



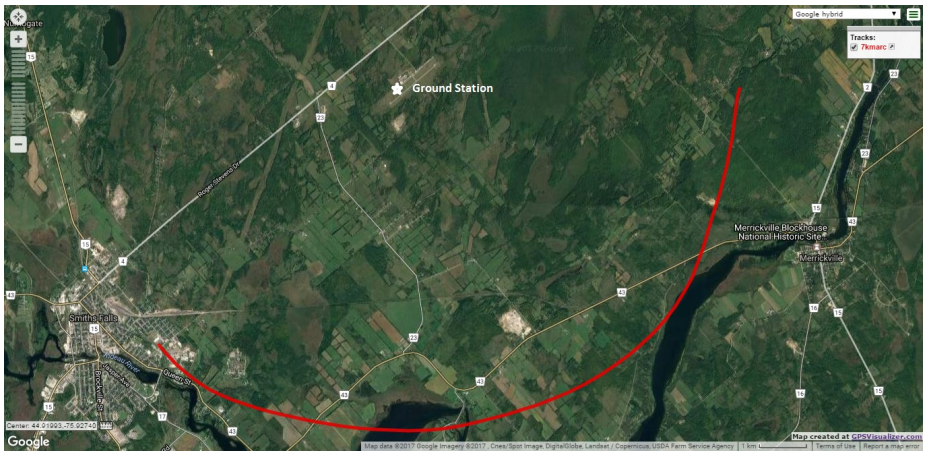
(b) 7 km Line

Figure 5.11: Aerial images of two of the flights from the first night where a quantum signal was successfully exchanged. In each photo, the aircraft moved from left to right. The white star signifies the ground station at Smiths Falls–Montague Airport. Photos produced using GPSVisualizer.com, map data ©2017 Google, imagery ©2017 Cnes/Spot Image, DigitalGlobe,Landsat/Copernicus,USDA Farm Service Agency, TerraMetrics.

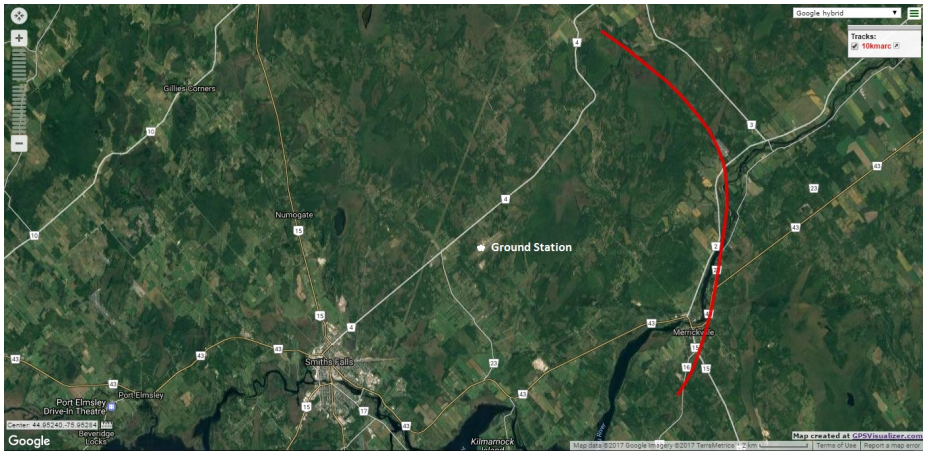
(a) 3 km Line

(b) 3 km Arc

Figure 5.12: Aerial images of two of the flights from the second night where a quantum signal was successfully exchanged. In each photo, the aircraft moved from left to right. The white star signifies the ground station at Smiths Falls–Montague Airport. Photos produced using GPSVisualizer.com, map data ©2017 Google, imagery ©2017 Cnes/Spot Image, DigitalGlobe,Landsat/Copernicus,USDA Farm Service Agency, TerraMetrics.



(a) 7 km Arc



(b) 10 km Arc

Figure 5.13: Aerial images of two of the flights from the second night where a quantum signal was successfully exchanged. In each photo, the aircraft moved from left to right. The white star signifies the ground station at Smiths Falls–Montague Airport. Photos produced using GPSVisualizer.com, map data ©2017 Google, imagery ©2017 Cnes/Spot Image, DigitalGlobe,Landsat/Copernicus,USDA Farm Service Agency, TerraMetrics.

until the coarse pointing software locked on the beacon lasers, and then they were turned off for the remainder of the link. This prevented any background light generated by the aircraft entering the detectors and causing noise in the QKD signal.

At one point in the second night, the VN-300 unit stopped producing GPS and attitude information, which prevented the coarse pointing software from working. As well, we could no longer determine the reference frame of the receiver, which is necessary for the polarization compensation. The backup described above was utilized and the pointing software was switched to receive inertial data directly from the airplane, allowing the experiment to continue. After a few minutes, the VN-300 system resumed working and the program was switched back to use its input.

In total, seven of the 14 airplane passes over the ground station successfully established a quantum signal link. Issues, including minor equipment failures (e.g., a loose beacon camera lens as described earlier) and accidental controller misconfiguration, particularly hampered link establishment during the first night—two of the seven attempts were successful.

The second night had a considerably better link establishment rate—five of seven attempts. The two failures on the second night were both straight line flight attempts. The likely cause of these flights failing was the fixed orientation of the WiFi transceiver on the aircraft being poor for this geometry, particularly at the beginning of a pass. The WiFi transceiver was pointing so it would have a large vertical spread (relative to the side of the plane) but it was limited in the fore-aft direction (relative to the plane). It was mounted this way as the various ground distances would require different angles and a large vertical spread ensured we could capture many distances. This, however, meant that acquiring the classical link was difficult when approaching at an angle not perpendicular to the ground station. For the circular flights, this was not a problem because the transceiver was always pointing directly at the ground station. A few adjustments were made in-air for the flight paths to accommodate more time for key to be established and the problems that the line links were having with the WiFi (We did select a backup device in case the WiFi link failed. However, due to the successful trial runs during the day flight and previous airborne test of classical links, it was not implemented).

The moon was near full during the tests, but it was also located behind the airplane, relative to the ground station, and consequently no noticeable background light was introduced. Covers were installed over the windows on the starboard side of the airplane to block the moonlight from entering the cabin. During the second night, there was a layer of cloud cover at approximately 3 km, well above the flight altitude, provided another block for the moon light. The ground station site also had background lights from the nearby

Date	Max Temp [°C]	Min Temp [°C]	Avg. Temp [°C]	Temp During Experiment [°C]	Dew Point [°C]
12/09/16	23.7	6.6	15.2	13.6	8.4
13/09/16	25.9	8.8	17.4	19.2	15.4
14/09/16	19.7	6.3	13.0	9.7	6.9
15/09/16	18.2	4.0	11.1	7.4	7.2
16/09/16	22.6	3.5	13.1	13.0	9.3
17/09/16	22.2	13.7	18.0	20.0	19.6
18/09/16	26.1	16.1	21.1	18.2	17.6
19/09/16	25.3	14.6	20.0	17.3	16.8
20/09/16	27.0	13.1	20.1	22:00–16.3 23:00–15.7	22:00–7.4 23:00–7.0
21/09/16	27.0	7.9	17.5	22:00–18.3 23:00–16.6	22:00–11.4 23:00–11.2
22/09/16	26.5	11.5	19.0	14.8	14.0
23/09/16	17.2	6.3	11.8	9.0	7.9

Table 5.2: Maximum and minimum temperatures during the flight campaign as well as the temperatures and dew points during the flights (or equivalent times). The temperature and dew points for days when flights were not conducted are at 22:00 EDT. Weather data from Environment Canada (station near Kemptville) and www.friendlyforecast.com (station near Kingston).

buildings. Due to the moon and this surrounding light (reflections from Smiths Falls lights off the clouds on the second night) the ground station site was fairly illuminated (personnel could walk around and see without flashlights).

During the preparation week before the flights, the weather at the ground station location was very difficult for tests as there was a large amount of fog and dew forming rapidly on the equipment (even with dew busters active). Fortunately, the two nights during which flights took place were extremely calm, no fog was visible, and dew was not a problem for the equipment. Weather data for the two week campaign period can be found in Tables 5.2 and 5.3.

The wind during the first night made it difficult to attempt the planned slower speeds as it was from behind the aircraft. The evenings in the first week where the minimum temperature was quite low were the more problematic nights as they were also clear (allowing the equipment to radiate to space and cooling it faster) which caused a majority of the

Date	Total Precipitation [mm]	Wind Speed
12/09/16	0.2	SSW 11 km/h
13/09/16	0.0	SW 12 km/h
14/09/16	0.0	N 13 km/h
15/09/16	0.0	N 5 km/h
16/09/16	0.0	SSE 29 km/h
17/09/16	14.8	SSW 27 km/h
18/09/16	7.0	SSE 15 km/h
19/09/16	0.2	WSW 7 km/h
20/09/16	0.0	22:00–WNW 18 km/h 23:00–WNW 15 km/h
21/09/16	0.0	22:00–SSW 8 km/h 23:00–N 1 km/h
22/09/16	0.8	SSW 7 km/h
23/09/16	6.3	N 14 km/h

Table 5.3: Precipitation and wind speeds during the flight campaign. Precipitation is the daily total and wind speeds are at 22:00 EDT unless otherwise stated. Weather data from Environment Canada (station near Kemptville) and www.friendlyforecast.com (station near Kingston).

dew problem. Fortunately the cloud cover during the last flight night helped keep ground temperatures warmer, preventing the formation of dew on the equipment.

Chapter 6

Airborne Quantum Key Distribution Results and Analysis

Notes

Parts of this chapter are adapted or used from material published on June 6, 2017 as [156]:

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

Some material also was published in a project report submitted to the National Research Council of Canada [162].

6.1 Analysis and Results

Secret key was extracted out of six of the seven successful passes. Circular-arc passes allowed the demonstration of longer durations for key exchange, compared to straight-line passes, as the receiver telescope held a relatively constant position during the pass, making link establishment and pointing easier. Straight line passes, however, are much more representative of a satellite passing over a ground station, as they simulate the change in angular speed that would be experienced during such a pass. The maximum angular rate is reached when the airplane is closest to the ground station for that type of pass. The successful passes can be seen in bold in Table 6.1.

First Night	Second Night
5 km Arc	**5 km Arc**
5 km Arc	3 km Line
7 km Arc	**3 km Line**
5 km Arc	**3 km Arc**
5 km Line	7 km Line
3 km Line	**7 km Arc**
7 km Line	**10 km Arc**

Table 6.1: Flight distances and types for the 14 passes between the two night flights. The flights where a quantum signal was successfully received are bold.

6.1.1 Physical Performance

The greatest angular rate measured by the GPS flight parameters was 1.28 °/s at a distance of 3 km (arc). This angular rate is greater than many overflying LEO spacecraft, which have angular velocities closer to 0.72 °/s for a 600 km orbit, as baselined for QEYSSat. The International Space Station, which has an orbit closer to 400 km, has an angular velocity of 1.2 °/s.

Due to wind and turbulence in the air, it was difficult to keep the airplane at exactly 1.5 km altitude and at the desired distance, as well as maintain an exact speed. Figure 6.1 demonstrates the ground-speed, angular rate relative to the ground station, and the altitude of the airplane for the 3 km arc pass.

Tables 6.2 (first night) and 6.3 (second night) summarize the seven passes where quantum signal was successfully transmitted to the receiver aboard the aircraft. Passes typically lasted a few minutes, with the aircraft traveling at 198 km/h to 259 km/h. To quantify pointing performance, the typical pointing error is defined as the measured distance of the beacon spot from the calibrated reference point on the camera image, discarding times when the motors had just begun tracking. The mean typical pointing error at the transmitter varied from 0.001 33° to 0.0220° over the passes; at the receiver, it was 0.0630° to 0.126°. The receiver's FPU measured pointing errors similar to the pointing error of the transmitter, between 0.002 39° to 0.0127°, where the deviation was measured from the center of the quad-cell sensor. (These values are used in the link analysis model, described in Chapter 4.)

Figures 6.2 to 6.5 show the observed results for the successful link passes, including the motor speed of the transmitter in the horizontal axis, the coarse- and fine-pointing errors

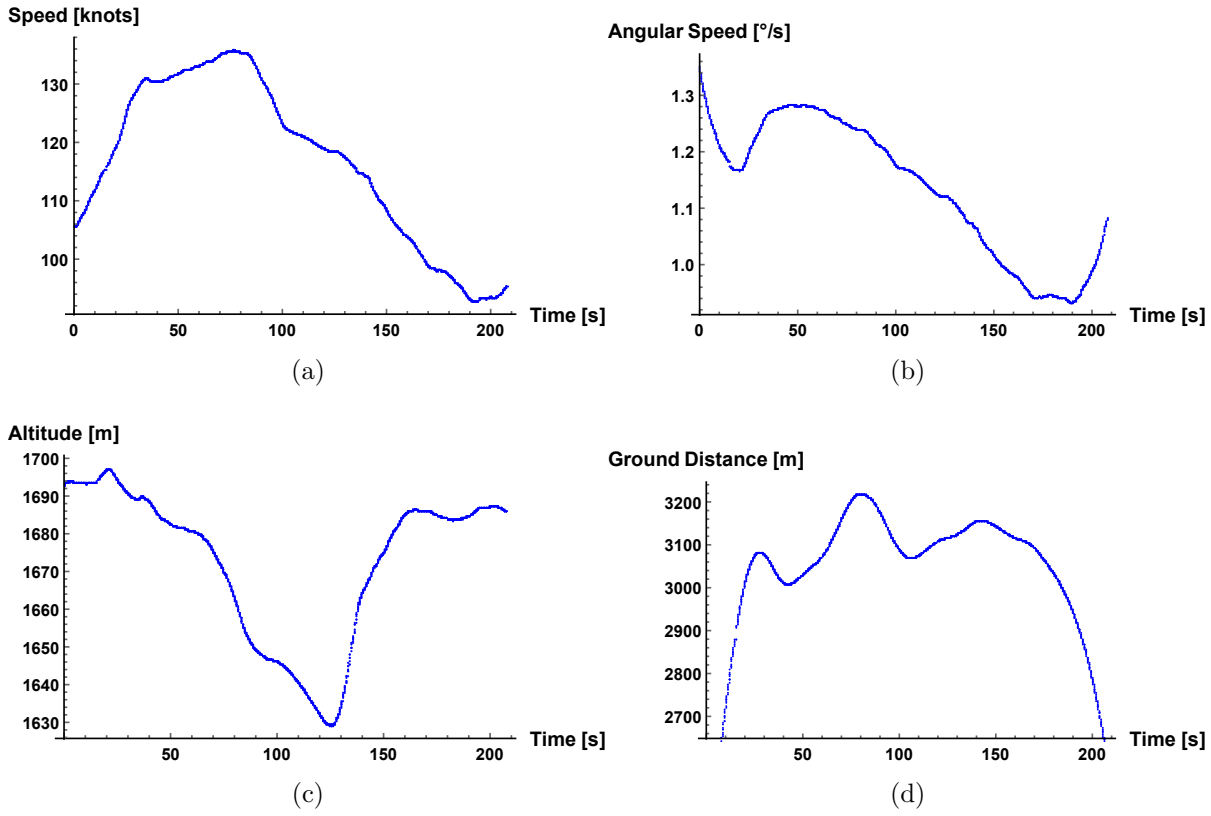


Figure 6.1: Flight parameters for the 3 km arc pass as recorded by the VN-300. Single photons were being received from approximately 40 s to 200 s. (a) Airplane ground-speed in knots showing an increase and decrease in speed due to the wind. (b) Angular speed as referenced to the ground station. (c) Altitude of the airplane above sea-level. (d) Distance as measured from the point on the ground directly below the airplane to the ground station.

Pass Parameter	5 km arc 1 2016-09-21 2:57:45	7 km line 2016-09-21 3:30:45
Classical link duration [s]	288	172
Quantum link duration [s]	235	158
Mean speed [km/h]	208	200
Maximum angular speed [°/s]	0.76	0.45
Transmitter pointing error (10^{-3})[°]	22.0	4.85
Receiver pointing error (10^{-3})[°]	125	126
Receiver fine-pointing error (10^{-3})[°]	2.73	9.98
Source QBER [%]	5.08	3.58
Signal QBER [%]	13.13	5.24
Decoy QBER [%]	19.54	11.1
Theoretical loss [dB]	52.1	41.6–44.8
Mean measured loss [dB]	48.0	51.1
Error correction efficiency	1.4	1.16
Signal-to-noise threshold	0	1500
Sifted key length [bits]	152508	95710
Secure key length [bits]	None	9566*

Table 6.2: Summary of data from passes during the first night (Sept 20, 2017) where a quantum link was established. All times are UTC. Except where indicated (*), secure key lengths incorporate finite-size effects.

Pass Parameter	5 km arc 2 2016-09-22 1:15:23	3 km line 2016-09-22 2:19:33	3 km arc 2016-09-22 2:24:45	7 km arc 2016-09-22 2:42:16	10 km arc 2016-09-22 2:57:42
Classical link duration [s]	352	34	170	210	289
Quantum link duration [s]	250	33	158	206	269
Mean speed [km/h]	198	236	216	259	212
Maximum angular speed [°]	0.75	1.0	1.28	0.60	0.37
Transmitter pointing error (10^{-3})[°]	1.33	3.42	2.91	1.58	2.82
Receiver pointing error (10^{-3})[°]	63.0	86.5	89.8	78.6	87.2
Receiver fine-pointing error (10^{-3})[°]	No data	2.62	2.39	3.01	12.7
Source QBER [%]	3.32	2.66	4.37	2.80	3.39
Signal QBER [%]	3.42	2.96	5.20	2.96	3.30
Decoy QBER [%]	6.13	6.35	7.93	5.97	8.46
Theoretical loss [dB]	28.1	33.3–35.1	30.9	32.1	39.9
Mean measured loss [dB]	34.5	39.5	34.4	39.4	42.6
Error correction efficiency	1.33	1.4	1.18	1.46	1.27
Signal-to-noise threshold	2000	1000	1000	2000	2500
Sifted key length [bits]	5212446	853066	5102122	2348086	1175317
Secure key length [bits]	867771	71648	44244	200297	70947

Table 6.3: Summary of data from passes during the second night (Sept 21, 2017) where a quantum link was established. All times are UTC. Secure key lengths incorporate finite-size effects.

at the receiver, the calculated time of flight of the quantum signal from the transmitter to the receiver, the rate of detections of all four DM channels combined, and the QBER of the signal. The time of flight can easily be translated into distance through

$$D = c \times t, \tag{6.1}$$

where D is the distance from the transmitter to the receiver (neglecting the small sections of optical fiber at each end, as well as the air index of refraction, which is very small), c is the speed of light, and t is the time of flight. A circular pass should demonstrate a constant time of flight and a line pass should demonstrate a smoothly decreasing time of flight followed by an increase after the plane passes the closest point to the ground station. Due to wind, it is very difficult to keep the plane at an exact radius for the circular passes, so there is some deviation in the time of flight.

In several of the trials, the inset shows the elapsed time from initial classical link acquisition, to acquisition of the spot on the beacon camera, to beacon lock and tracking, and finishing with receiving photon detections. Many of these elapsed times were around 10 s, with the best (the 7 km arc) having a time of 8 s. It is important to get the tracking lock and signal exchange as quickly as possible. With a satellite, there is only a limited amount of time to perform the quantum optical exchange, and the more time used for initiating tracking, the less time is available for the exchange.

For the 3 km arc pass, the fine pointing performance can be found in Figure 6.6. From the figure, we see that while the unit was tracking, its performance was very similar to the truck testing as well as the in-lab testing. The sections on both sides of the plot show where there was no beacon signal and the unit was not tracking. The beacon power plot shows the slight change in the beacon power throughout the arc, averaging around -42 dBm. The measured power of the beacon lasers was $\sim$40 mW, implying $<$4 µW was reaching the beacon detector. This falls within the acceptable range of the FPU of 0.01 µW to 17 µW.

In contrast, during the 10 km arc pass, the beacon power was fluctuating near the threshold of sensitivity of the FPU. This can be seen in Figure 6.7. This was due to the relatively large divergence of the beacons for such a distance. If this divergence could be reduced, or the power increased (both very feasible tasks), the pointing would likely work well at this distance and further.

The mean measured loss of the quantum link during the flights varied from 34.4 dB to 51.1 dB. Indeed, in the experiment, a number of passes were conducted with the transmitter intentionally slightly defocussed so as to avoid saturating the detectors, which occurred at approximately 20000 counts per second in the worst channel. Consequently, the experimental losses we observed are generally higher than the theoretical losses. The difference

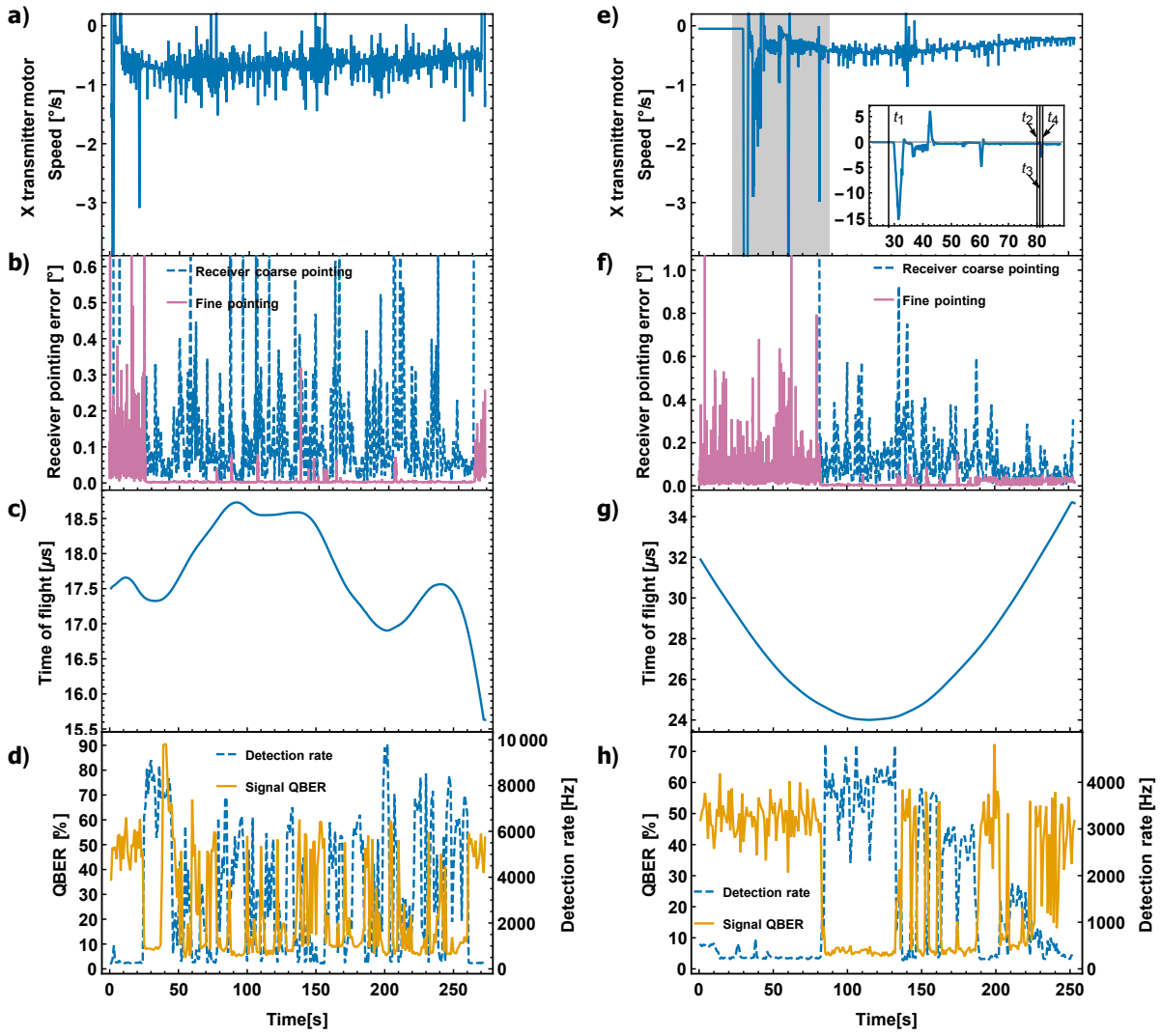


Figure 6.2: Results for the 5 km arc pass (left) and the 7 km straight-line pass (right) from the first night. a) and e) show the speeds of the azimuthal (coarse) motor at the transmitter. The inset in e), corresponding to the shaded portion, shows the motor speed during initial acquisition, with times t_1 through t_4 identifying establishment of the WiFi link, identification of the beacon spot, lock to the beacon spot, and first counts received, respectively. b) and f) show coarse- and fine-pointing performance at the receiver. Where there are no coarse pointing data (e.g., at the beginning of a pass), no beacon spot was found in the camera image. This corresponds with large fluctuations in the fine-pointing deviation—in the absence of beacon light, the unit operates on electrical noise generated at the QD. c) and g) show the estimated time of flight of the photons from the transmitter to the receiver (used in event time-correlation), calculated from per-second GPS coordinates at each site. The smooth curve in g) is particularly characteristic of the straight-line pass, with a similar shape to that of a satellite pass. d) and h) show the total detection rates at the receiver and the QBER of the signal.

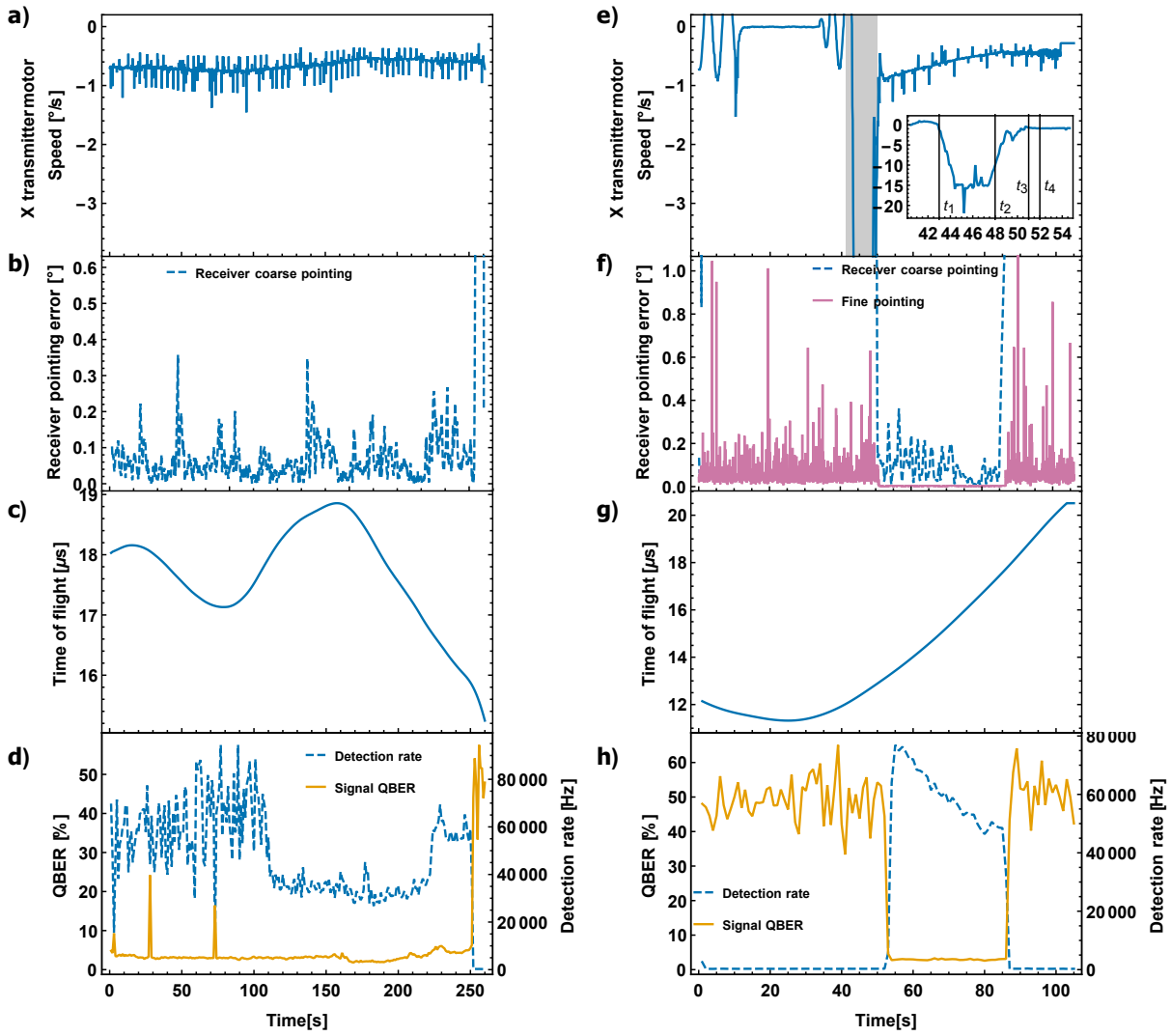


Figure 6.3: Results for the 5 km arc pass (left) and the 3 km straight-line pass (right) from the second night. a) and e) show the speeds of the azimuthal (coarse) motor at the transmitter. The inset in e), corresponding to the shaded portion, shows the motor speed during initial acquisition, with times t_1 through t_4 identifying establishment of the WiFi link, identification of the beacon spot, lock to the beacon spot, and first counts received, respectively. The oscillation prior to this in a) is from a spiraling search state of the pointing software. f) shows coarse- and fine-pointing performance at the receiver, whereas b) only shows the coarse pointing as the FPU was being optimized and no fine pointing data was being recorded. Where there are no coarse pointing data (e.g., at the beginning of a pass), no beacon spot was found in the camera image. This corresponds with large fluctuations in the fine-pointing deviation—in the absence of beacon light, the unit operates on electrical noise generated at the QD. Sub-figures c), d), g), and h) follow those of Figure 6.2.

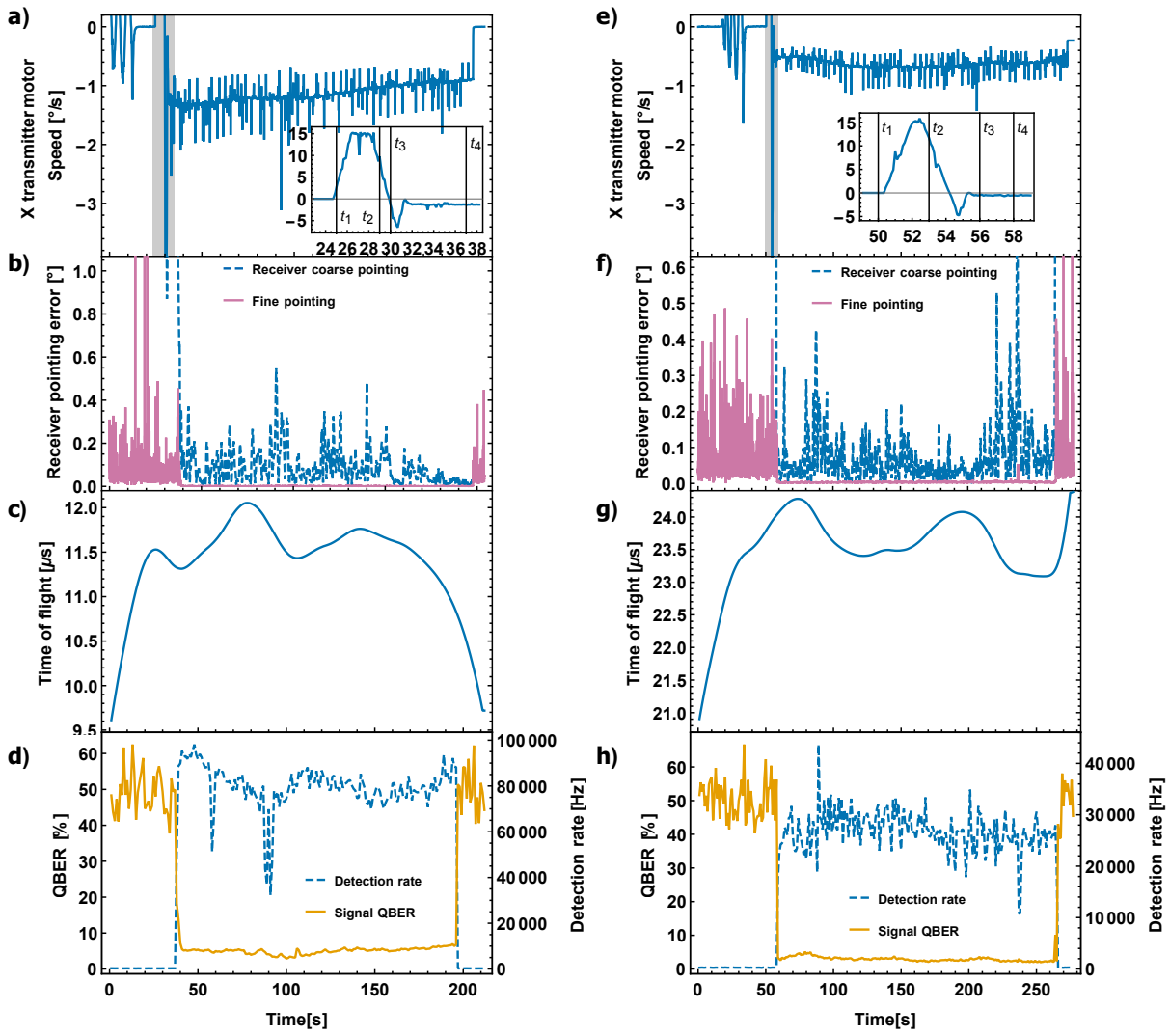


Figure 6.4: Results for the 3 km arc pass (left) and the 7 km arc pass (right) from the second night. a) and e) show the speeds of the azimuthal (coarse) motor at the transmitter. The insets, corresponding to the shaded portions, show the motor speed during initial acquisition, with times t_1 through t_4 identifying establishment of the WiFi link, identification of the beacon spot, lock to the beacon spot, and first counts received, respectively. The oscillation prior to this in a) is from a spiraling search state of the pointing software. b) and f) show coarse- and fine-pointing performance at the receiver. Where there are no coarse pointing data (e.g., at the beginning of a pass), no beacon spot was found in the camera image. This corresponds with large fluctuations in the fine-pointing deviation—in the absence of beacon light, the unit operates on electrical noise generated at the QD. Sub-figures c), d), g), and h) follow those of Figure 6.2.

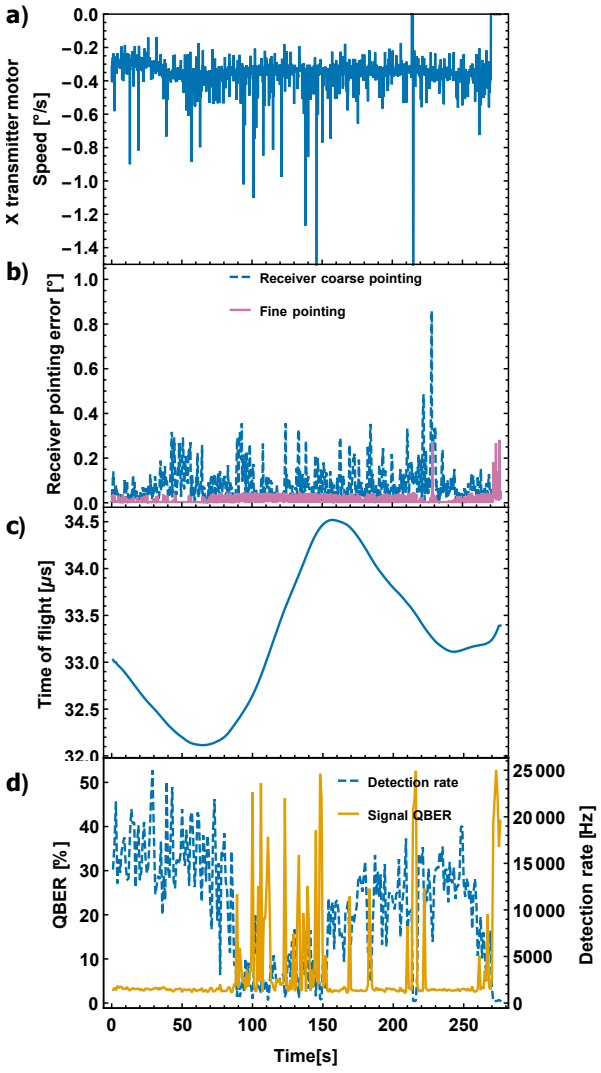


Figure 6.5: Results for the 10 km arc pass from the second night. a) shows the speed of the azimuthal (coarse) motor at the transmitter. b) shows coarse- and fine-pointing performance at the receiver. c) shows the estimated time of flight of the photons from the transmitter to the receiver (used in event time-correlation), calculated from per-second GPS coordinates at each site. d) shows the total detection rates at the receiver and the QBER of the signal.

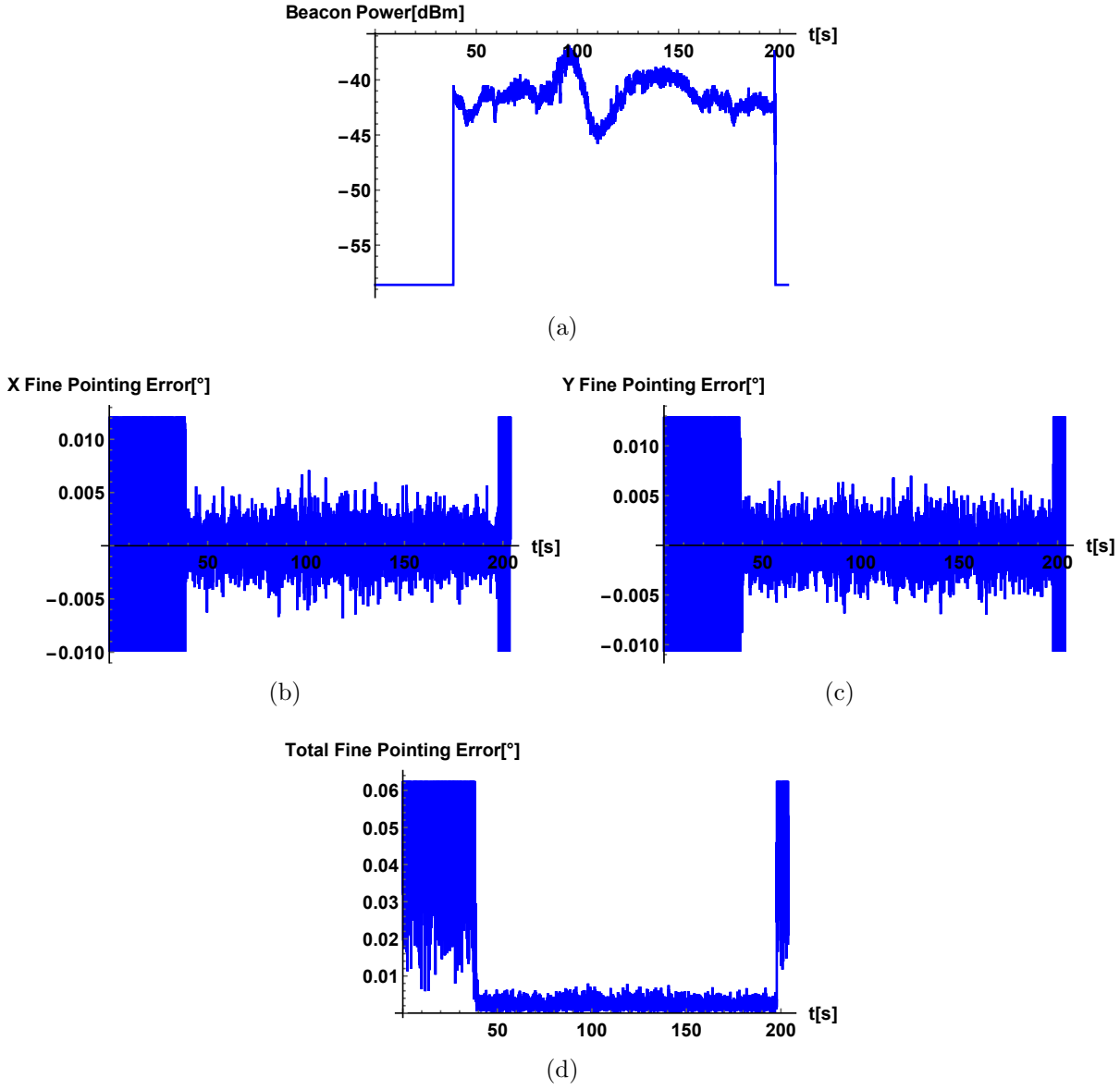


Figure 6.6: Receiver fine pointing performance for the 3 km arc pass. (a) Beacon power measured in dBm. The power being sent was approximately 40 mW, implying about 5 orders of magnitude loss. The wide divergence of the beacons relative to the quantum signal explains why this loss is greater than that for the quantum signal. (b) The x error of the fine pointing. (c) The y error of the fine pointing. (d) The total fine pointing error. The edges demonstrate where no beacon was found; once the tracking is active and locked, it is very stable throughout the pass.

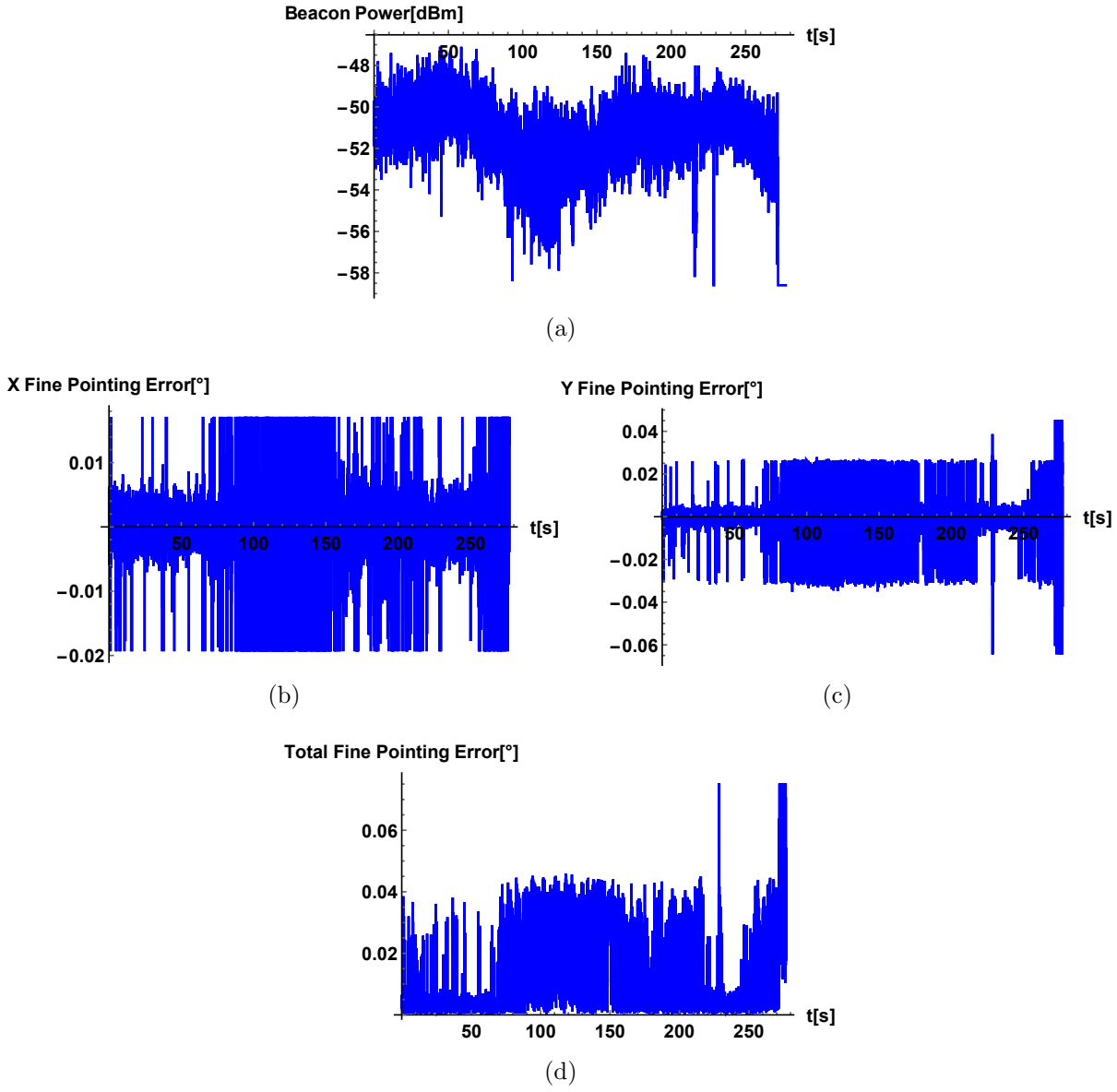


Figure 6.7: Receiver fine pointing performance for the 10 km arc pass. (a) Beacon power measured in dBm. The power being sent was approximately 40 mW, implying about 6 orders of magnitude loss. The wide divergence of the beacons relative to the quantum signal explains why this loss is greater than that for the quantum signal. This power level was on the lower threshold of performance for the device, so dropouts occurred frequently. (b) The x error of the pointing. (c) The y error of the fine pointing. (d) The total fine pointing error. Since the power was below the threshold of operation frequently, the tracking performance dropped frequently.

between the theoretical loss of an arc pass and the minimum theoretical loss of a line pass at the same nominal distance is due to varying pointing accuracy experienced for each pass, as well as the actual ground distance and altitude deviating from nominal.

The source's intrinsic QBER, as predicted by the polarization correction system, varied between 2.66 % and 5.08 % for each pass. The black cloth shielding the FPU, IOA, and fibers at the receiver led to typical total background detection rate of ≈285 Hz.

The QBER measured at the receiver dropped to a few percent upon optical link lock, and rests at ≈50 % due to the random noise of background detections at all other times. For passes where secure key was generated, the QBER varied from 2.96 % to 5.24 %. The received QBER during the first night flight was observed to be higher than for the second night, possibly due to an issue with the wave plate motorized stage controller in the polarization compensation system.

6.1.2 Data Analysis

For the QKD analysis, a signal-to-noise (SNR) filter [163] is implemented which assesses the total counts in each 1 s frame of data and discards any frame with counts less than a threshold, prior to distilling key bits. Thresholds between 1000 and 2500 were chosen, depending on the pass. Background detection rates at the beginning and end of the pass are sufficiently low that those frames are discarded by the SNR filter. Some drop-outs can be seen, for example, in Figure 6.2h), and these frames are also discarded by the SNR filter.

Secure key bits are generated from the data collected during each pass using algorithms tailored for the asymmetric processing resources that would be available with a satellite platform [164]. These algorithms consist of source and receiver event time-correlation (performed at the ground station), error correction utilizing LDPC codes, and privacy amplification via reduced-Toeplitz-matrix two-universal hashes. A screen-shot of the QKD software analysis program GUI can be seen in Figure 6.8.

The software operates multiple stages of processing, first collecting time-tagged event data independently at Alice (transmitter) and at Bob (receiver). For Bob, these data identify the detected time of arrival and polarization measurement outcome. For Alice, they identify the WCP source generation events, and monitor the status and quality of the output signal. For technical reasons, the pulse states (intensity and polarization) we generate follow a randomized sequence, 1000 pulses long, which repeats. Alice's time-tags correspond to the start of each sequence period, and the software interpolates between adjacent start time-tags to estimate the time of transmission for each state.

Figure 6.8: A screen-shot of the QKD software developed in the Quantum Photonics Laboratory by Brendon Higgins, Nick Gigov, and Chris Erven. The counts are monitored for each state and the QBER and loss are also measured and displayed. The histogram in the bottom right displays the algorithm searching for the correct peaks between Alice's and Bob's time-tags The blue peak shows the correct alignment has been found for the one second frame of data.

In addition to these data, Alice and Bob also record GPS time and position coordinates once per second. These are aligned to a pulse per second (PPS) signal produced by the GPS, which is time-tagged and used for subsequent timing correlation analysis. All of Alice's time-tags are referenced to a 10 MHz clock produced by the GPS receiver, which is phase-locked to the GPS signal. We consider this our reference clock. Bob's time-tags, on the other hand, are referenced to a stable free-running on-board oven-controlled crystal oscillator (OCXO) running at a nominal 100 MHz.

The QKD software processes the data in per-second frames, defined by the PPS tags. For each per-second chunk, the next processing stage, time correlation, starts with Bob transmitting time-tags and a random subset of measurement outcomes, to Alice. Taking only a subset is necessary for the QKD protocol, as it facilitates estimating the error rate prior to error correction, without revealing the remaining bits which are subsequently used to generate secure keys. At Alice, each of Bob's per-second time-tag frames are brought together with her own corresponding chunks (identified by the GPS time information), and coincidence analysis is performed.

To begin coincidence analysis, the QKD software makes two adjustments to Bob's time-tags. First, a time-of-flight estimate based on the recorded GPS positions is subtracted. Second, because the actual oscillation of Bob's clock differs slightly from the nominal rate, a clock-drift compensation must be applied. To accomplish this, the QKD software performs a statistical analysis and optimization algorithm based on the expected periodicity of aggregate detections (as determined by the periodic WCP source). This produces a clock-drift rate (CDR) factor k_{CDR} that is applied to Bob's time-tags.

To complete the timing analysis, the QKD software produces a coincidence histogram (as seen in Figure 6.8) which counts the number of coincidences (within a given time window) of Alice's transmission events and Bob's detection events as an additional small delay is varied. Because of the periodicity of the WCP source, this histogram is also periodic, because Alice and Bob's tags must align for each source pulse period. To identify the correct delay from these multiple peaks, the software searches for the peak possessing the smallest number of vacuum detections. Only the correctly matched peak will have a low number of coincident counts for the times where Alice transmitted the vacuum state (i.e., when Alice did not send any optical power). If a signal or decoy peak was aligned to a vacuum pulse, within the one second data chunk in question, Bob will receive real photons when he should have received nothing.

Finding the center of this correct peak gives an optimized delay with precision on the order of 1 ns. All the coincidences in a window around that peak are then selected and used in the next QKD processing stages, which include measurement basis sifting, error

correction, and privacy amplification.

To ensure security, the uncertainty due to the finite number of samples used to estimate link parameters must be taken into account. Of the six passes from which key could be extracted, five yielded secure key including these finite-size effects (where we use the common ten-standard-deviation heuristic to bound parameter estimates [52]). The remaining pass had too few counts and could only generate secure key assuming no finite-size effects. The QKD key data were evaluated and studied offline after the flight. Although the software does have the capability of performing this step in real-time, it requires more resources and processing time on the ground, which we did not want during the limited flight time. It also would have used more bandwidth on the WiFi, which could have inhibited the GPS transmissions and led to failure of the coarse pointing, which will not be an issue with a satellite implementation.

6.2 Aside: Feasibility of Single-Photon Ranging

In addition to performing QKD, the data from the airplane experiment was analyzed to determine the feasibility of using it for the task of ranging. In the trials, the photonic quantum source had a 400 MHz emission rate of photons with randomly encoded states of polarization and intensity. These signatures could be used for *near-continuous* ranging measurements between the ground and the aircraft.

In quantum communication, as the airborne quantum receiver (e.g. on an aircraft or satellite platform) moves over the optical ground station (OGS), the range between them will be a function of time. This will directly relate to a certain transfer time of the photons, as they travel between the ground and receiver. When comparing the times of the received photons with the emission times at the source, the value of time of flight for each photon can be estimated to an accuracy of < 0.5 ns as long as the creation and detection events are correlated to better than 0.5 ns.

Through several steps we determine the time-of-flight function in time, T, making the following assumptions:

1. For practical reasons, all recorded times will be expressed in an absolute time scale, such as in terms of UTC in order to ensure consistency of the experimental data.

2. Both the ground and airborne system have highly precise frequency standards with an absolute precision of 1e-9, used to ensure the recorded time-tags are referenced to

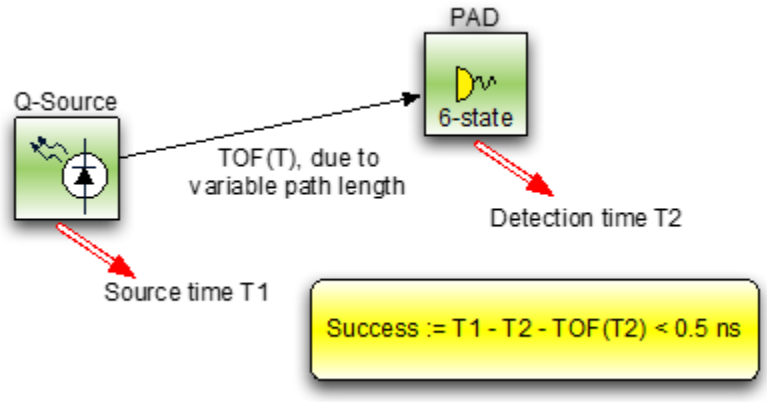


Figure 6.9: Concept of the photon correlation; Detection time T_2 must be related to the Source emission time T_1 within 0.5 ns. This allows one to know the path length for each photon to better than 0.5 ns. (Diagram created by Thomas Jennewein.)

a highly stable time base. This can conveniently be provided through GPS-steered clocks.

3. Both the ground and airborne systems have access to an absolute time reference (UTC) to better than 100 ns, and the capability to relate the recorded events (time-tags) with respect to UTC. This can best be provided through GPS receivers.

If we are able to exploit the timing information from the photons while performing QKD for ranging, it could potentially lead to *near*-continuous secure ranging. This is also a first step towards applications such as Quantum Illumination [165–167] and Quantum Radar [168].

6.2.1 Data Collection

Using the existing QKD software described previously, we are provided with coincidence data from which we can extract photonic times of flight. Minor modifications to the software facilitated output of data relevant to time of flight just after coincidence analysis. For the time of flight analysis, Alice and Bob's state and measured time-tags (before adjustments), for every identified coincidence, and Alice and Bob's PPS time-tag and optimized CDR, for each per-second chunk of data are extracted.

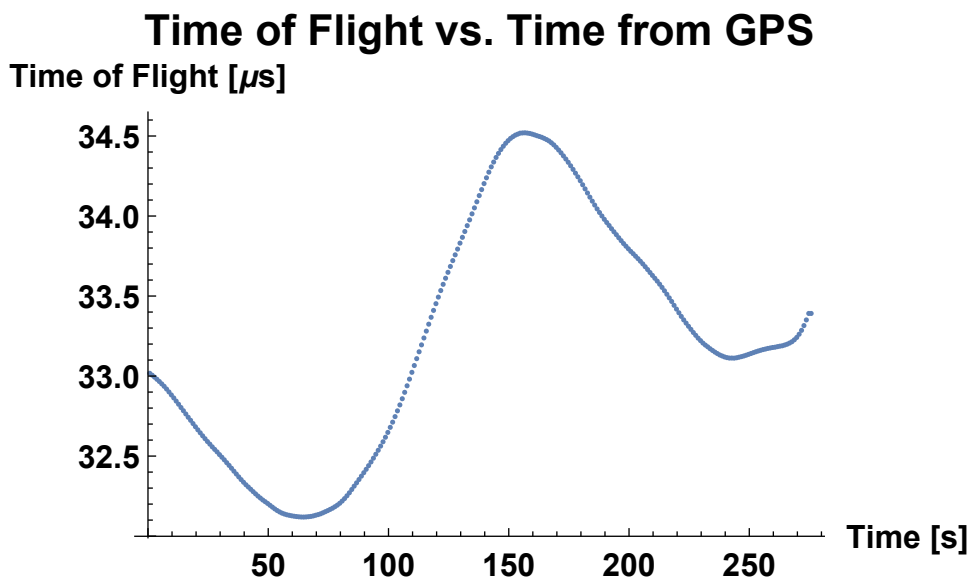


Figure 6.10: Time of flight during the 10 km arc flight, calculated from the GPS coordinates of the optical ground station and the airplane.

6.2.2 Analysis

The first step of the analysis is to take the data which is output in binary format from the QKD algorithm and convert it into text format for analysis. In order to observe an advantage of the single photons for ranging, if any, GPS location data is used which is collected at 1 Hz for comparison. A plot of the time of flight calculated from the GPS coordinates for the 10 km arc is shown in Figure 6.10. This is a plot of the full ∼275 s run.

To calculate the time of flight from the photons, the value of Alice's time-tag corresponding to a received photon at Bob is subtracted from the value of Bob's time-tag for the corresponding sent photon. These time-tags are each referenced to a PPS signal from a GPS receiver at each site (with < 100 ns accuracy).

In order to align the per second chunks of coincidence data, and in lieu of an accurate reference clock at Bob, it is necessary to first correct Bob's times for the clock drift. Determining this clock drift independent of the actual time of flight of the photons is not straightforward. For this analysis, it is assumed that the clock at Bob is precise and stable over the time of the data collection, and can therefore be modeled as a constant over all the per-second chunks of data.

The appropriate value of k_{CDR} (as described in Section 6.1.2) must be determined. To do this, two different approaches are considered. The first averages over each per-second

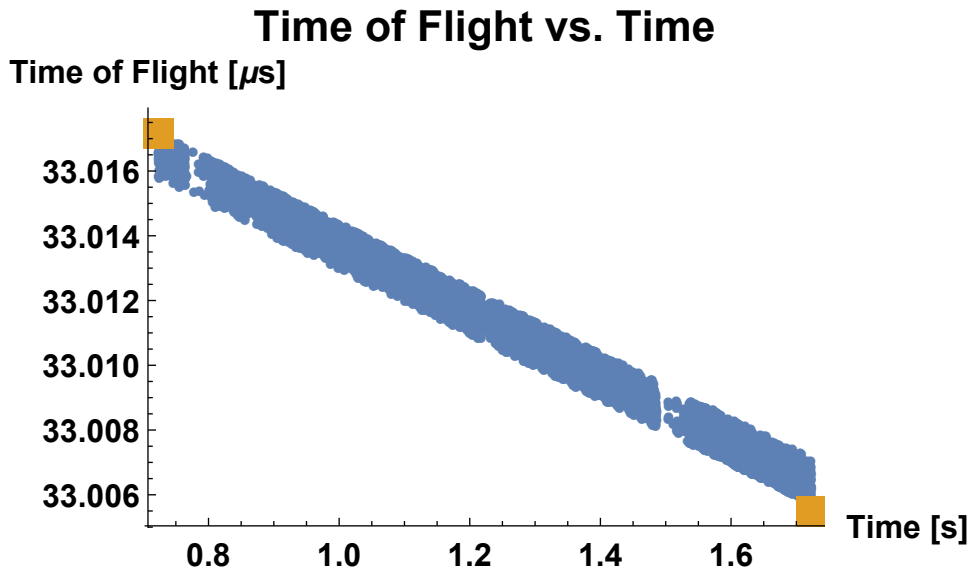


Figure 6.11: Times of flight over one second of data during the 10 km arc flight. Orange squares at either end are times of flight calculated from GPS coordinates of the optical ground station and the airplane. Small blue circles are times of flight of each of the signals received by Bob. In this plot there are 12770 photons recorded.

optimized CDR value, $k_{\mathrm{CDR},i}$, found by the QKD software's analysis:

$$k_{\mathrm{CDR}} = \frac{1}{N}\sum_{i}^{N} k_{\mathrm{CDR},i}. \tag{6.2}$$

The second method takes the ratio of Alice's mean measured time between each PPS to Bob's mean measured time between each PPS,

$$k_{\mathrm{CDR}} = \frac{\frac{\sum_i^N (t_{\mathrm{Alice\ PPS},i+1} - t_{\mathrm{Alice\ PPS},i})}{N}}{\frac{\sum_i^N (t_{\mathrm{Bob\ PPS},i+1} - t_{\mathrm{Bob\ PPS},i})}{N}}. \tag{6.3}$$

The actual PPS times are linked to GPS, and taking the mean smooths the inherent (uncorrelated) PPS jitter. This approach was chosen for the following analysis. The time of flight is calculated by applying the clock drift correction factor to each of Bob's time-tags and subtracting Alice's corresponding time-tags,

$$T_i = k_{\mathrm{CDR}} \times t_{\mathrm{Bob},i} - t_{\mathrm{Alice},i}. \tag{6.4}$$

Figure 6.11 shows one second of data taken from the 10 km arc flight. This is the first second of data as referenced to Alice's PPS start time, and it demonstrates the 12770 received photons within that second and their changing times of flight. The width of the

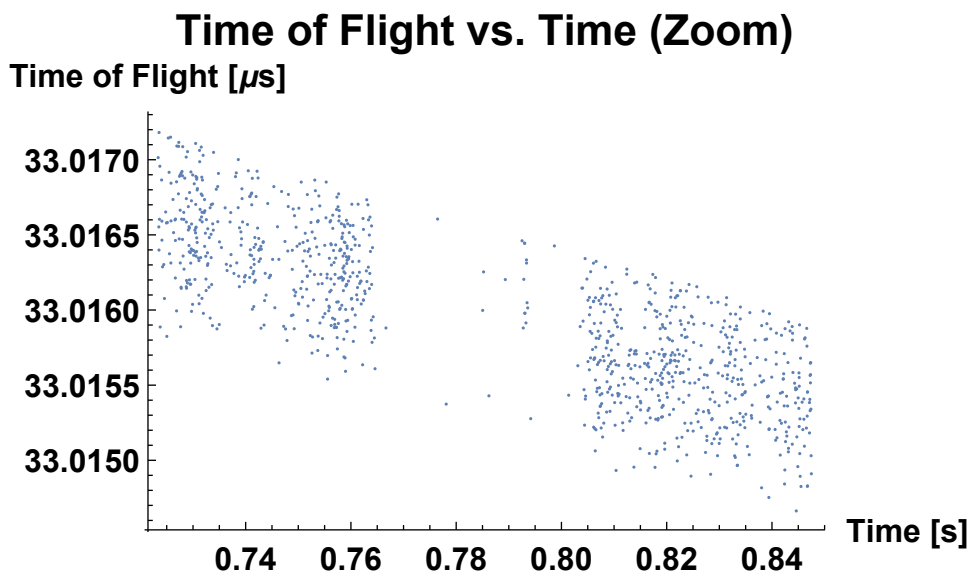


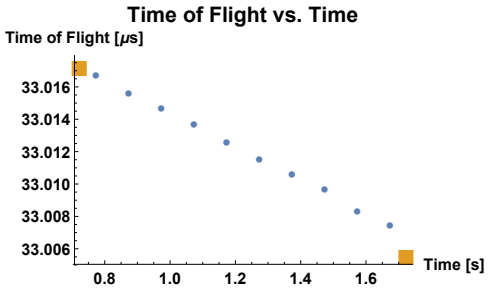
Figure 6.12: Times of flight within just over 0.1 s; there were 1000 photons received. This section also shows a drop out in data collection and a recovery a very short time later. The width of the time of flight spread is the coincidence window for correlating Alice's sent photons with Bob's received photons, which here was 1.5 ns.

spread in times of flight can be attributed to the coincidence window which the QKD software looks for to correlate photons received at Bob with those sent by Alice. For a majority of the flight paths, this value was 1.5 ns. Figure 6.12 shows a smaller time section where we can see a drop out in the data collection when the beacon signal was temporarily lost.

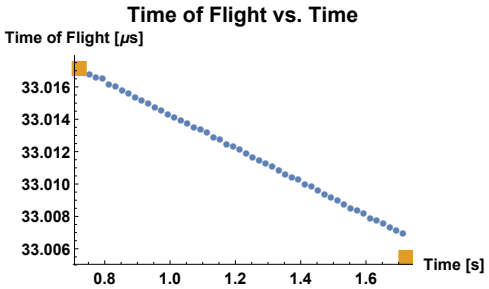
It is straightforward to calculate the distance represented by this time of flight by using Equation 6.1, and for this section of data distance was approximately 9.9 km.

The time of flight information can be separated into various bins for each time of flight point between the GPS points to get varying levels of resolution. The smaller bins will have less photons per bin, but will have a higher resolution as long as there are enough photons to fill the bins. Figure 6.13 shows this technique for 10, 50, 100, and 1000 bins, corresponding to 0.1 s, 0.02 s, 0.01 s, and 0.001 s respectively. In order to find the time of flight value for each bin, the mean is taken of the points within that bin. In the 1000 bin plot, we can begin to see the spread due to the coincidence window appearing as the number of photons per bin on average starts to approach 10.

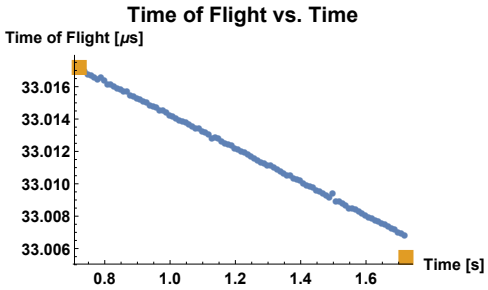
When the number of photons is larger, such as in Figure 6.14 with approximately 80000 photons, we can see that even when 1000 bins are used (approximately every 0.001 seconds in one bin) the data are very uniform.



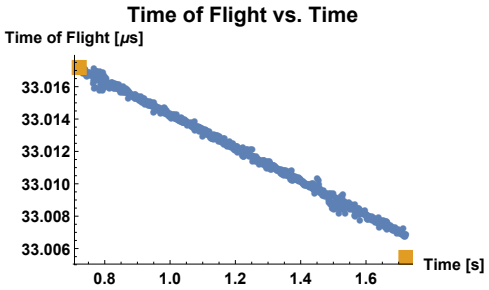
(a) 10 bins, average 1277 photons per bin.



(b) 50 bins, average 255 photons per bin.

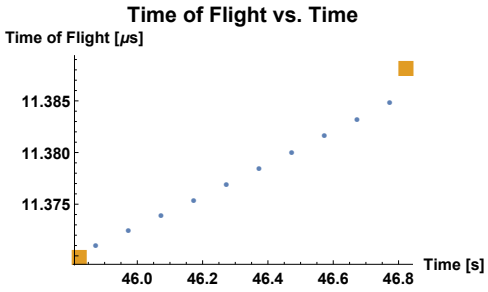


(c) 100 bins, average 128 photons per bin.

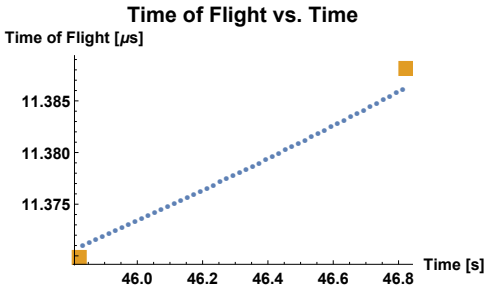


(d) 1000 bins, average 13 photons per bin.

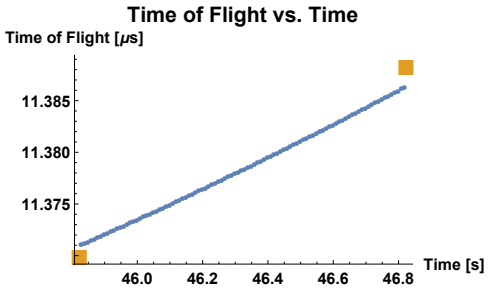
Figure 6.13: Times of flight over one second of data separated into various numbers of equally sized bins for the 10 km arc flight. As fewer bins are used, more photons appear in each bin. By increasing the number of bins, the time resolution is increased. There are a total of 12770 photons in this one-second period.



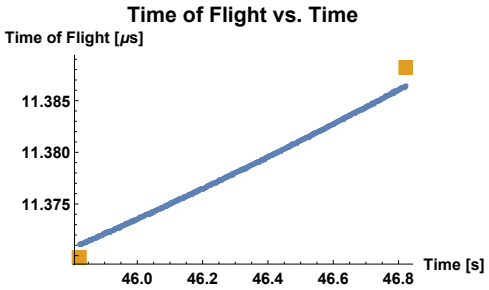
(a) 10 bins, average 8035 photons per bin.



(b) 50 bins, average 1607 photons per bin.

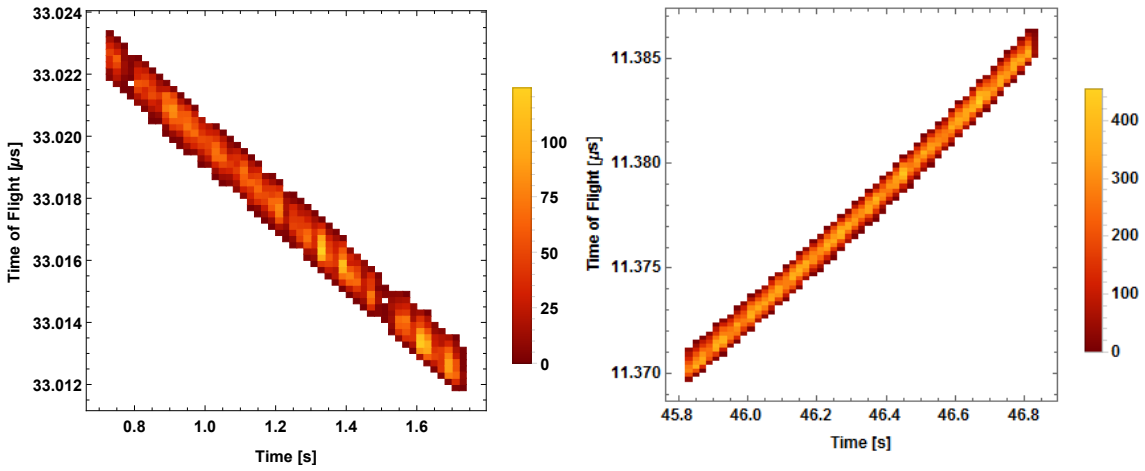


(c) 100 bins, average 803 photons per bin.



(d) 1000 bins, average 80 photons per bin.

Figure 6.14: Times of flight over one second of data separated into various numbers of equally sized bins for the 3 km arc flight. As fewer bins are used, more photons appear in each bin. By increasing the number of bins, the time resolution is increased. There are a total of approximately 80000 photons in this one-second period.



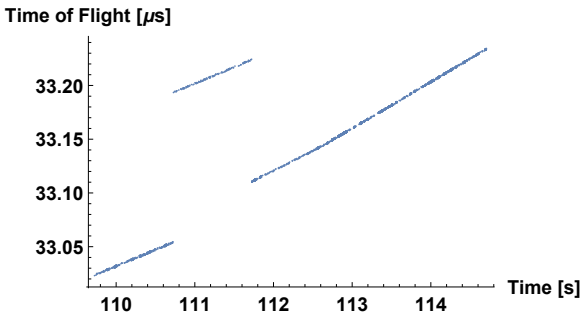
(a) (b)

Figure 6.15: Heat maps for time of flight data over one second. The correlated photon rate is higher in the center of the band. (a) 10 km arc flight with approximately 12000 photons. (b) 3 km arc flight with approximately 80000 photons. Each bin is 0.01 s.

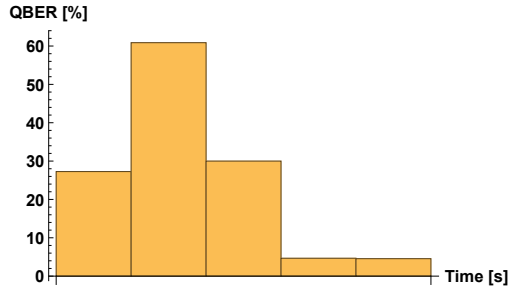
As mentioned previously, the spread of the photon times of flight is directly related to the coincidence window of the analysis. By having a larger coincidence window, one allows for more detections, but also increases this spread, as well as the noise level. Figure 6.15 demonstrates a heat map of the time of flights. Note that the majority of measurements occur in the center of the curve, with much fewer counts occurring at the edge of the coincidence window.

When there is a drop in counts and the background is dominant, the QKD software can often have trouble aligning the appropriate coincidence peak between Alice and Bob. This can often be seen as a shift in the observed time of flight as well as a poor QBER. This quantity measures the correlations between the sent and observed states. In the QKD protocol, we look for this value to be around 5 % or less. A QBER of around 50 % would mean completely uncorrelated data. This parameter can also be used to gauge whether the photons we are aligning between Alice and Bob are the correctly correlated combination. Figure 6.16 shows a plot where the number of photons drops to background levels and the QBER increases. The counts then increase again and show a drop in the QBER and re-align along the real time of flight curve.

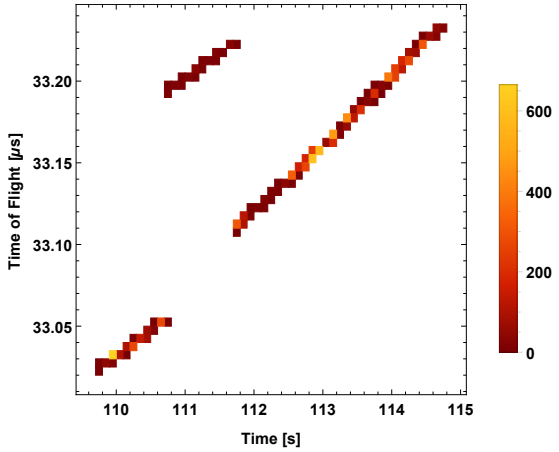
In Figure 6.17 an increase in the QBER for one second where the counts dropped but not to completely background level was observed. The QBER is still well below 50 % which means there are still signal photons present. The software was able to align the proper PPS but there were still too few counts to have good statistics for a good QBER.



(a)

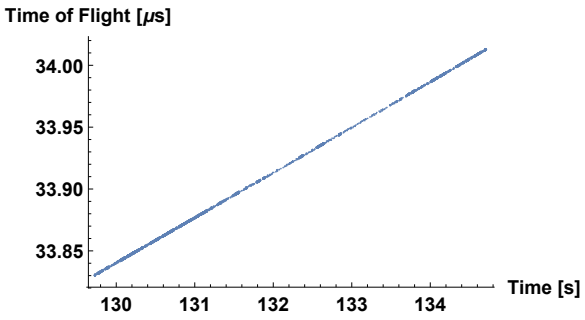


(b)

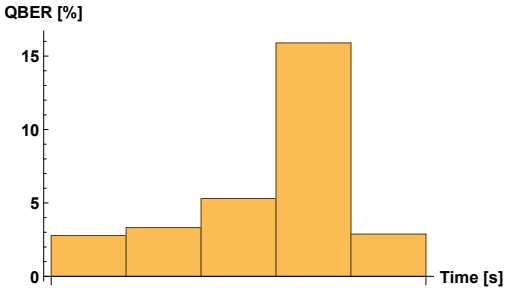


(c)

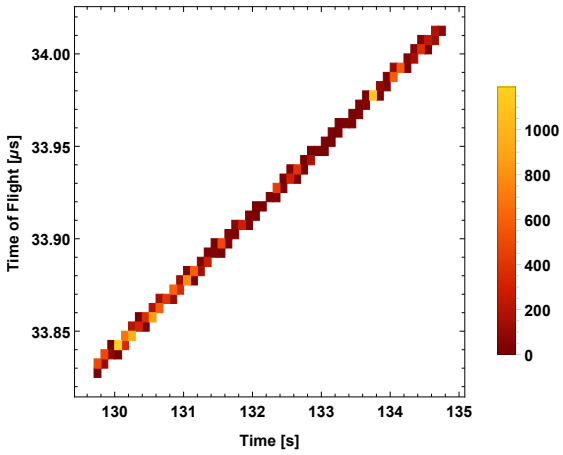
Figure 6.16: (a) The shift when the coincidence peak was improperly correlated between Alice and Bob due to primarily background counts. (b) The jump in QBER when the counts are low and the data is uncorrelated. Once the counts return, the QBER drops back to an operable level. (c) The heat map showing the low number of counts for the aberrant section, and the increase in counts towards the latter portion of the plot. Each second contains 1818, 176, 1149, 3529, and 2342 counts respectively.



(a)



(b)



(c)

Figure 6.17: (a) The time of flight data. (b) The jump in QBER when the counts are low and the data is uncorrelated. Once the counts return, the QBER drops back to an operable level. (c) The heat map showing the increase in counts towards the latter portion of the plot. Each second contains 7206, 3908, 1673, 407, and 3722 counts respectively.

With just a few thousand photons, a QBER which allows for the generation of key can be achieved. The background level is approximately 200 counts per second, and as shown in Figure 6.16, 2300 photons can easily be correlated.

One final piece would be to compare the frequency at which this data performs vs. a traditional Light, Detection, and Ranging (LiDAR) system. Since LiDAR requires a pulse to reach the object and return before the next pulse is sent, it is limited by the time of flight of light to the object and back. For the 3 km link one second collected roughly 80000 photons thus operating at around 80 kHz. A LiDAR system for the same distance (assuming an average of 11.380 µs time of flight) would have a maximum frequency of 44 kHz thus we could achieve almost twice the frequency of a traditional LiDAR system.

6.3 Discussion

The details of path-to-flight modifications necessary to construct space-suitable versions of the receiver components varies. Some elements present on the CDPU daughterboard, for example, will need to be replaced with radiation-hard equivalent versions. Or, for the IOA, glues designed for low out-gassing must be used. Sensitivity of the Si-APDs in the DM to proton radiation in orbit is of particular note, as such radiation can significantly increase dark counts. However, strategies including cooling and thermal annealing [169], as well as laser annealing [170], are capable of mitigating these effects, and a space-suitable prototype DM implementing these strategies is being developed.

For pointing to a satellite from the ground, initial acquisition will likely not have a real-time classical communication link to exchange position data. In this case, however, predictions of the satellite position at the time when a link is to be established can be used, as the orbital trajectory of a satellite is predictable with far greater accuracy than the flight path of an airplane. In this context, point-ahead is necessary to ensure that the quantum beam is coincident with the satellite when it arrives, owing to the satellite's motion during the time of flight of the optical signals. A fine-pointing for the transmitter system would likely also be required to achieve sufficient accuracy over the significantly larger transmission distance. For the aircraft, this was not necessary.

One advantage of the up-link approach is source flexibility. While this demonstration only used a WCP source, QKD using entangled photon pairs generated at the appropriate wavelength will produce equivalent results under a BBM92-style protocol [171], with one photon of each pair measured on the ground. To support this, no aspect of the receiver prototype need be modified. Initial studies into an entangled photon source at

785 nm are currently underway with preliminary results showing brightness on the order of 6×10^5 pairs/s/µW [162].

Although the ranging data gained from the airborne experiments shows great correlation to the time of flight as well as very high resolution (down to 1 ms), the interesting part lies in that the channel was effectively secured with QKD. Not only were the photons used for ranging, but they also performed QKD at the same time potentially making the ranging data secure and preventing manipulation or modifying the signals. Although, a full security analysis needs to be performed before the security can be fully determined.

6.4 Conclusion

Through these experiments, we were able to successfully demonstrate QKD to a satellite receiver payload prototype on an aircraft moving at up to 1.28 °/s. The pointing and tracking system was able to establish and maintain an optical link with milli-degree precision over 3 km to 10 km distances while BB84 decoy-state signals were sent across the channel to the aircraft at similar angular speeds to a LEO satellite. Our custom FPU, IOA, DM, and CDPU, along with the other commercial components, all performed on the aircraft to generate secure keys, of tens to hundreds of kilobits in length, in various flight scenarios, including the straight-line paths approximating the apparent trajectory a LEO satellite. With source intrinsic QBER typically 2 % to 4 % and post-processing algorithms representative of what would be achievable with a satellite platform, we extracted finite-size secure key for many of the tested passes.

The aside on single-photon ranging showed that the quantum receiver has a very high sensitivity, and it was able to extract ranging data even from short bins of 1 ms, and containing only about 10 photons. The random modulation of the laser source in polarization as well as intensity provided suitable unique labeling of the photons, such that the correlations between received photons and the high-speed emission source (at 400 MHz) is verified.

Chapter 7

The NanoQEY Mission: Ground to Space Quantum Key Distribution Using a Nanosatellite

Notes

Parts of this chapter are adapted from material published in 2014 as [172]:

T. Jennewein, C. Grant, E. Choi, C. Pugh, C. Holloway, JP. Bourgoin, H. Hakima, B. Higgins, and R. Zee. The NanoQEY mission: ground to space quantum key and entanglement distribution using a nanosatellite. *Proc. SPIE*, 9254:925402–925402–6, 2014.

Some material was also published in a report submitted under a FEDDEV contract [173].

7.1 Introduction

The Nano Quantum EncrYption satellite (NanoQEY) is a proposed demonstration nano-satellite which will show the feasibility of implementing QKD between two ground stations on Earth using a trusted node approach with an optical up-link. One of the main objectives of NanoQEY is to eliminate the necessity for a fine pointing system (such as would be required by QEYSSAT [88]), which will reduce cost and planning time for the satellite. The smaller volume and mass of a nano-satellite vs. a micro-satellite will also force the system to be more compact and simplified. Since the satellite is only used for photon collection and data processing, it is not necessary to have many of the complicated systems on board which would typically be required for a down-link

As mentioned above, one of the major systems used on many of the micro-satellite designs is a fine pointing system. This complicates the design and adds to the mass and power consumption of the payload. By eliminating this system, we greatly simplify the design of our device, enabling us to save time as well as financial cost. As a result, however, the ground stations will need to compensate for the lack of targeting on the satellite. These ground stations will have to have very fine pointing and tracking capabilities. The satellite also will require a larger field of view, which will increase the background light and diminish the performance. In this chapter, we look into the requirements of the NanoQEY payload.

7.2 Payload Design

The payload for NanoQEY, if chosen for a mission, could be implemented on the University of Toronto Institute for Aerospace Studies Space Flight Laboratory's (UTIAS SFL) Nanosatellite for Earth Monitoring and Observation (NEMO) bus [174]. This satellite bus has dimensions of approximately $40\,\text{cm} \times 26\,\text{cm} \times 20\,\text{cm}$, is comprised of magnesium alloy, and has a total mass of 15 kg, of which 7.5 kg would be the QKD payload. In order to determine the feasibility of the proposed model, there is a defined list of requirements that the satellite must fulfill. Many of the requirements for this payload come from previous studies into the QEYSSAT mission and have been transferred to this mission. Table 7.1 shows a sampling of the requirements studied in the initial phase of the project (further and more detailed requirements are confidential). Figure 7.1 shows a block diagram of the major components necessary for NanoQEY.

One of the major deviations from the QEYSSAT mission is that this payload will have a field of view of 0.4 degrees, but there will be no active tracking through the payload itself. The satellite will perform target tracking to assist with the pointing but the major targeting strategy will be implemented on the ground.

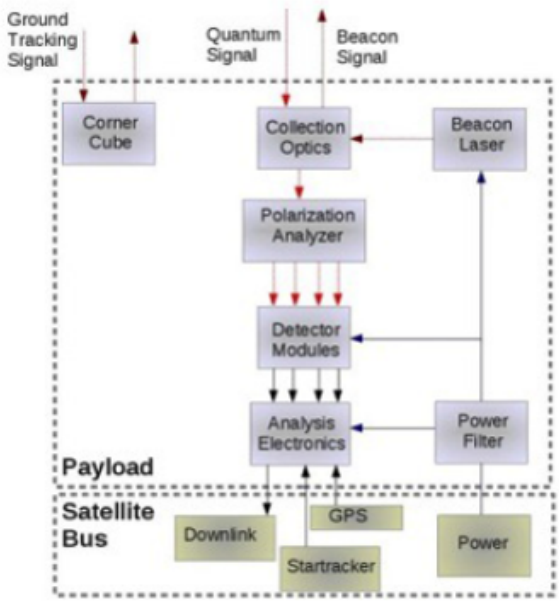


Figure 7.1: A block diagram of the important components of NanoQEY. The upper portion of the diagram contains the payload components while the lower portion contains the satellite bus components. The three major areas of the QKD payload consist of the optics (collection optics, corner cube, beacon laser, polarization analyzer), detection (detector module), and electronics (analysis electronics, power filter).

Title	Requirement
Spacecraft Accommodation	
Mass	The total mass of the payload shall not exceed 7.5 kg including margin and contingency.
Average Power	The average power consumption of the payload shall not exceed 8.5 W.
Peak Power	The peak power consumption of the payload shall not exceed 20 W.
Outer Dimensions	The outer dimensions of the payload shall fit within the contiguous volume defined in SFL drawing in the Interface Control Document.
GPS Connections	The payload shall have serial and PPS connections to the spacecraft's GPS receiver.
Environmental	
Operating Temperature	The payload shall be capable of operating within performance requirements at ambient temperatures ranging from −20 °C to +60 °C.
Radiation Environment	The payload shall be capable of operating within performance requirements during one year of exposure to a total ionizing dose of at least 1,000 rads/year.
Performance and Function	
Course Pointing	The payload shall achieve course pointing to an accuracy of 0.4°.
Polarization	The payload shall be capable of detecting single photons in two polarization bases (H/V and ±45°).
Time Tagging	The payload shall be capable of time-tagging single photon detections to a precision of 78 ps.
Star Tracker Data	The star tracker shall output data to the processor board of the payload to be included in the time-tagging files.
Optics	
Receiver Aperture	The aperture for the payload receiver telescope optics shall be no more than 15 cm in diameter.
Beacon Laser Aperture	The aperture for the payload laser beacon shall be no more than 15 cm in diameter.
Filter Center Passband	The payload receiver bandpass filter shall have a center passband of 639 nm with a FWHM of 1 nm or less.
Dichroic Beam Splitter	The dichroic beam splitter shall reflect at 810 nm and transmit at 639 nm.
Single Photon Detector	
Single Photon Detector Response	The single photon detector shall have a peak spectral response at 580 nm.
Single Photon Detector Quantum Efficiency	The single photon detector shall have a minimum quantum efficiency of 35% and a dark count rate of less than 30 cps.
Beacon Laser	
Beacon Laser Wavelength	The beacon laser shall operate in a wavelength range from 780 nm to 850 nm.
Beacon Laser Power	The power of the beacon laser shall be at least 1 W.

Table 7.1: Sampling of the payload requirements for the NanoQEY satellite.

Another obvious change from QEYSSAT is the mass restrictions. Having an upper bound on mass of 7.5 kg adds a stricter requirement on the equipment in the payload but should still be feasible. With the large field of view, it will be necessary for the ground station to be in a very dark location to reduce background light. A corner cube will be

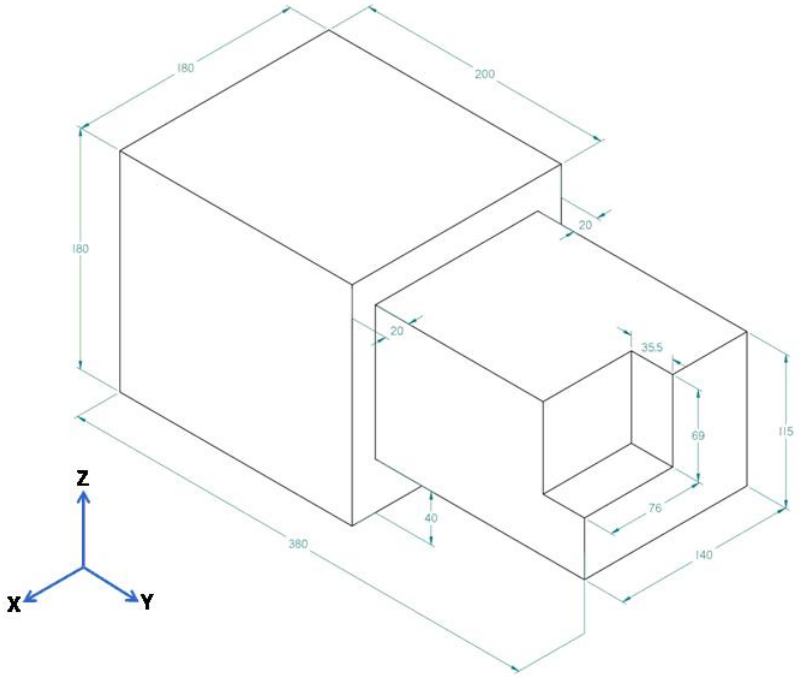


Figure 7.2: Payload volume provided by UTIAS SFL with dimensions in mm. The front half of the satellite measures 180 mm×200 mm×180 mm and the back half of the satellite measures 140 mm×180 mm×115 mm with a small portion removed from the back end to accommodate connections to the satellite bus.

installed on the front of the payload to allow the ground station to use a beacon laser to track the satellite.

Although the dimensions of the entire satellite are approximately 40 cm×26 cm×20 cm, the payload cannot occupy the entire space as the satellite itself also contains electronic and motion devices. The volume which can house the payload can be seen in Figure 7.2. This volume will put the constraints on the telescope as well as the QKD polarization analyzer.

The major components of the payload fall into three areas: optics, detection, and data processing. The optical portion of the payload includes a telescope and a passive polarization analyzer. The detection portion will consist of four single photon detectors. The data processing portion of the payload consists of the detection control and readout electronics, the time-tagging of the photon arrival, as well as the QKD software processor.

7.2.1 Optical Components

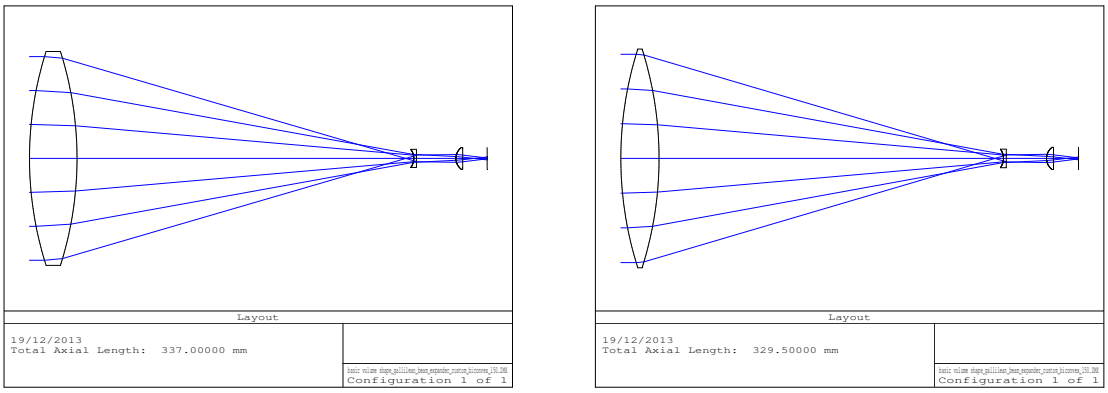
The optics portion of the NanoQEY payload can be broken down into two sections, the telescope portion for collecting photons from the ground, and the polarization analysis portion. Each of these are constrained by the volume of the payload, and the telescope also has to take into account the polarization effect on the photons as this cannot be altered for the protocol to work.

A further study also looked at the effect of implementing a sub-nanometer filter ($\approx$ 0.1 nm bandwidth) into the system to help reduce the background from the wider field of view. This study looked at: relativistic shift from satellite motion, bandwidth of the source, angular dependence of the filter, temperature variation, and performance in a vacuum environment. It was determined that it is feasible to use a filter with such a narrow bandwidth, however, temperature stabilization of the filter may be required.

7.2.1.1 Telescope

Although both reflective and refractive telescopes could conceivably fit within the payload volume, refractive telescopes have been chosen due to their simplicity and narrow field of view. Reflective telescopes also have more potential to affect the polarization of the photons as the curvature of the mirror is increased. With a simple refractive index telescope and a proper choice of material for the glass, this problem can be avoided. Fused silica glass is studied here as it is not birefringent and also works well in the radiation environment of space [175]. Although further study is necessary, this analysis provides a design that is potentially feasible for this concept.

The design proposed here is a three-lens system with a large primary lens, and two collimation or "eyepiece" lenses. The primary lens is biconvex and the second and third lenses are plano-convex and plano-concave respectively. The radius of curvature of the primary lens was determined to be approximately 266 mm by focusing a 150 mm diameter beam (the maximum size of the aperture limited by payload volume) into a 12 mm beam (the size of typical cube beam-splitters) using a second fused silica lens with a radius of curvature of 11.25 mm and diameter of 15 mm. This second lens was chosen based on the minimum radius of commercially available plano-convex lenses; it may be possible to obtain a smaller radius with custom optics, see Figure 7.3 for a Zeemax ray tracing image of the system. The space behind the final telescope lens, where the beam is collimated, extends for 29 mm, enough space to fit at least two cube beamsplitters. A third, 6 mm radius lens is used to focus the spot onto the detectors (the real system would have four of these placed in front of the detectors).



(a) (b)

Figure 7.3: Galilean beam expander systems with 150 mm diameter apertures. The two designs are differentiated by the minimum lens thickness at the edge. (a)The primary lens has a minimum thickness of 10 mm, a system length of 337 mm, and a weight of 768 g. (b)The primary lens has a minimum thickness of 2.5 mm and a system length of 329.5 mm and a weight of 661 g. The difficulty with the lens that has a smaller edge width is the robustness of the lens.

Both Keplerian and Galilean telescopes were considered. Keplerian telescopes require more space (an additional 25 mm in system length) to achieve the same magnification as Galilean telescopes due to the intermediate focus. In order to reduce the system length for Keplerian systems, shorter lens radii are required, however this increases the system weight, as shown in Figure 7.4. Total system weights are compared for minimum lens thickness of 2.5 mm and 10 mm. According to BMV Optics [176], a space-specialist optics manufacturing company, standard optics mounts for large optics require a minimum thickness of 10 mm, however we might be able to mount thinner optics for our design in order to reduce the mass.

Short radii of curvature on the primary lens lead to spherical aberration in our systems, however short radii allow for higher ratios of aperture to system length. Spherical aberration could be reduced using either custom aspherical lenses, or smaller opening apertures. In addition, systems with shorter radii of curvature lead to heavier optical systems. However, as the telescope weighs less than 0.8 kg, weight is unlikely to be an issue. Beam displacement can be minimized by tightening the focus of the second lens. As with the primary lens, however, this will lead to more spherical aberration.

Spot diagrams were computed using ray-tracing for fields at -0.4, -0.2, 0, 0.2, and 0.4

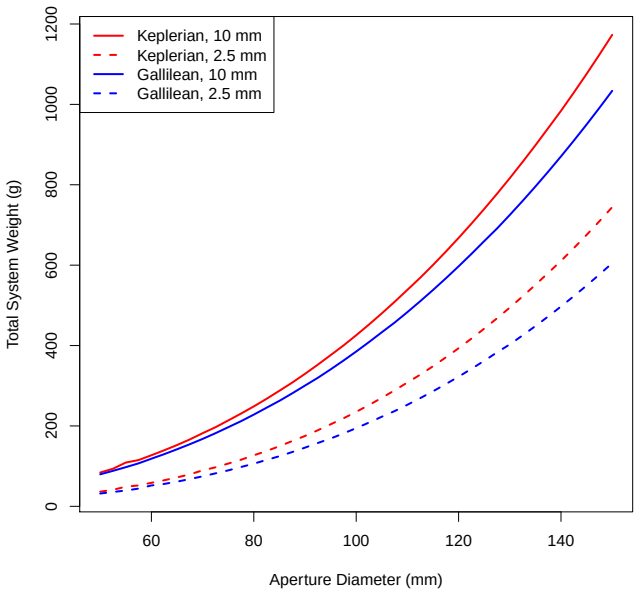


Figure 7.4: Total weight of the optics as a function of the aperture diameter, for Keplerian and Galilean systems, with minimum edge thicknesses of 2.5 mm and 10 mm. The Galilean systems weigh less than the Keplerian systems making them a more feasible option.

degrees. The spots are presented in Figures 7.5. The spot sizes are between 1.6 mm to 2.0 mm, and do not diverge from the center by more than 1.5 mm.

The field of view can be estimated from ray-tracing. A field composed of a rectangular grid of rays was traced through the system, and the fraction of rays that reach the image plane are counted for different input angles of the field. The fraction of rays passing through the system is plotted in Figure 7.6. The field of view from ray tracing is sufficient for our experimental requirements.

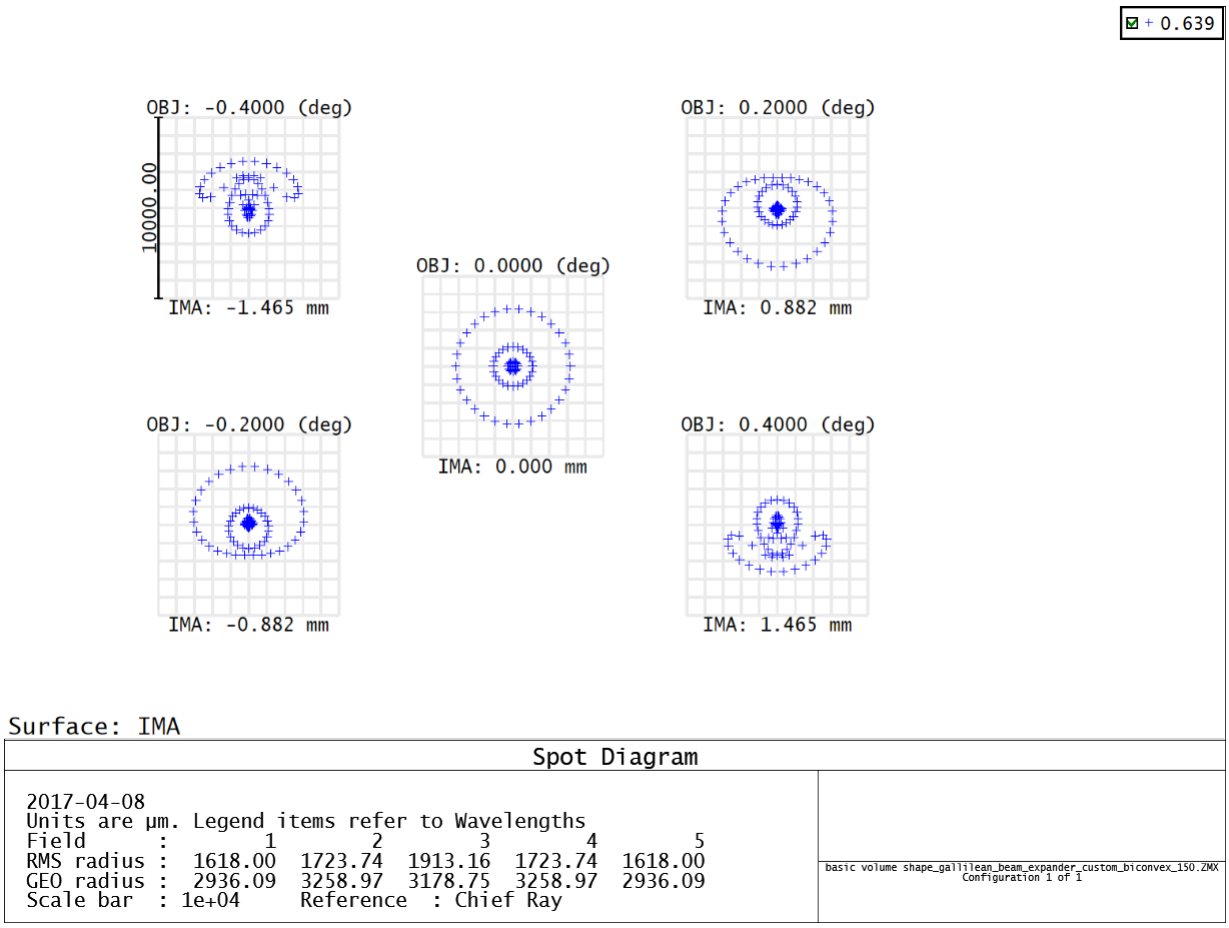


Figure 7.5: Spots in the image plane from the 150 mm aperture Galilean beam expander with a biconvex primary lens, and a minimum lens thickness of 10 mm. Shown are the spots created by fields at 0.2, 0.1, 0 (center image), -0.1, and -0.2 degrees. RMS radius is calculated by taking the RMS of the distance between the center and the rays, and GEO radius is calculated by constructing the smallest radius which encircles all rays. In this case, the RMS of the 0° field is approximately 2 mm, and the maximum deviation from the center is 1.5 mm.

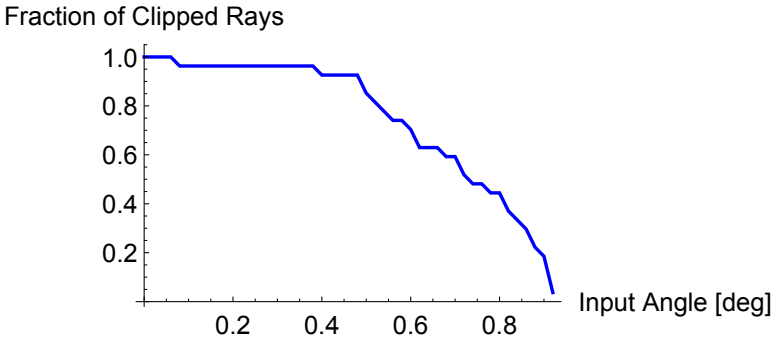


Figure 7.6: The fraction of the rays from a rectangular grid which reach the image plane from the aperture, versus the angle of the field, for the 150 mm diameter aperture Galilean beam expander systems. The transmission only drops off at around 0.4 degrees, resulting in a field of view sufficient for our mission concept.

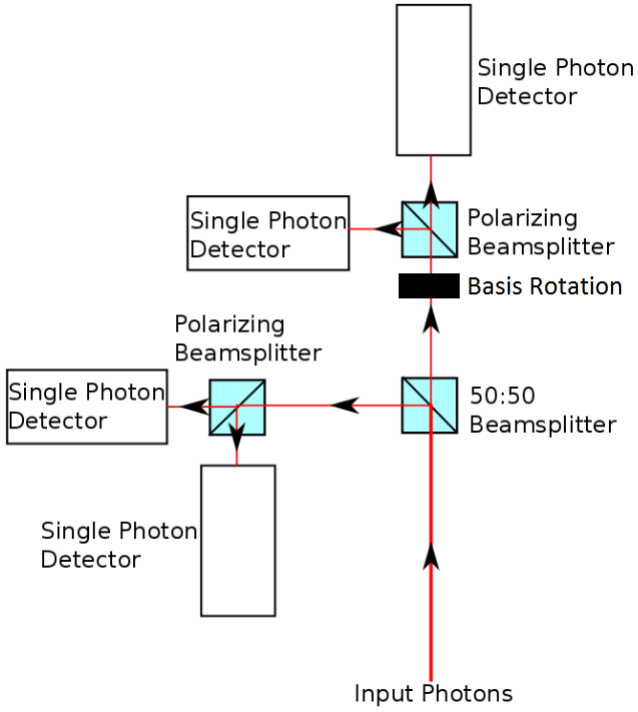


Figure 7.7: A simple model of a passive QKD analyzer. The 50:50 beam splitter chooses between the HV+ and DA× bases. The basis rotation is performed by a physical rotation of the polarizing beamsplitter by 45°.

7.2.1.2 Polarization Analyzer

The polarization analyzer will follow the second lens of the Galilean telescope. This system is used to analyze the QKD states sent from the ground station and is accomplished through a passive system. A simple model of the polarization analyzer can be seen in Figure 7.7. The system uses a 50:50 beamsplitter to randomly choose between the HV+ basis and the DA× basis. The HV× photons then pass through a polarizing beam splitter to be analyzed and sent to the detectors. The other arm must convert to the DA× basis, which can be accomplished with a half-wave-plate, but this would require another optical element that would require further study for use in a space environment. Instead, a simple 45° rotation of a polarizing beamsplitter will accomplish the same goal. This comes at the cost of increasing the complexity of the geometrical design.

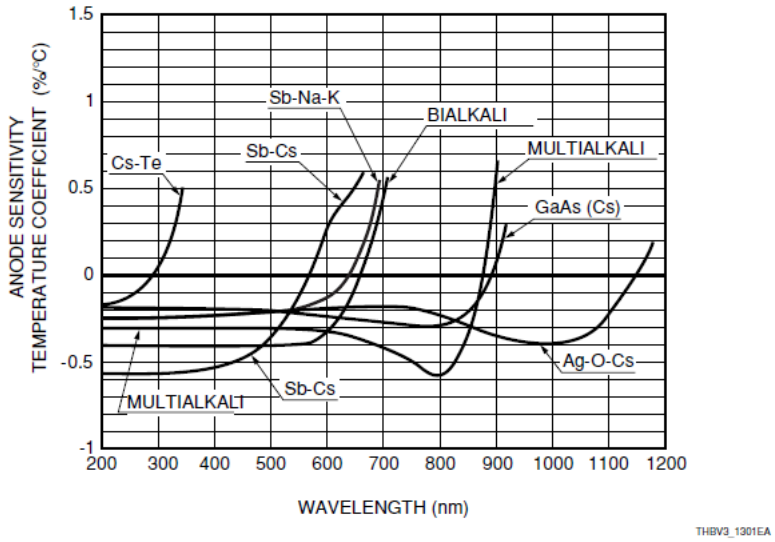


Figure 13-1: Temperature coefficients of photomultiplier tube photocathodes

Figure 7.8: Anode sensitivity temperature coefficients vs. wavelength for various PMT material types. Photo from the Hamamatsu PMT handbook [180].

7.2.2 Detection

The available volume, background radiation environment, and single photon detection performance must be taken into account in order to choose an appropriate detector. Both photomultiplier tubes (PMTs) and APDs have available modules capable of fitting into the payload volume. Both devices have been tested in space-like applications. PMTs have been space qualified for many missions [177, 178] and respond well to the radiative environment of space. They generally also have larger active areas. APDs have been studied in space-like radiation environments [169, 179], however this causes an increase in the dark count rate. For our particular scheme, we will be using free space detection which both devices are capable of. Taking into account these factors, PMTs are the more suitable detectors for this mission.

PMTs are quite sensitive to temperature and will need to be fairly well controlled and kept at a low temperature. The temperature coefficient of various PMT materials increases with longer wavelengths and can help guide the specific choice of PMT. Figure 7.8 shows the anode sensitivity temperature coefficients as a function of wavelength.

Cooling also reduces the dark current, which is important for achieving the low dark count rates required for our application. Figure 7.9 shows the anode dark current vs. temperature for common PMT varieties. Turning on the PMTs a few minutes prior to

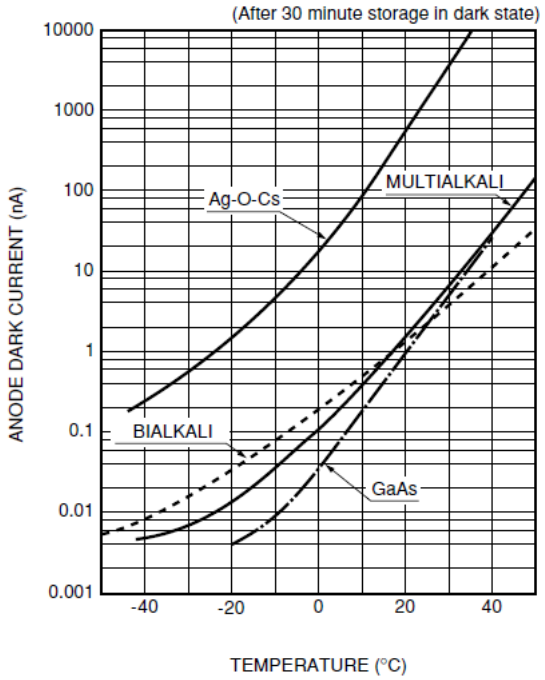


Figure 13-3: Anode dark current vs. temperature

Figure 7.9: Anode dark current vs. temperature for a few common varieties of PMT's. Photo from the Hamamatsu PMT handbook [180].

their operation will cause them to become thermally stable with the radiator and be stable in temperature for the pass duration.

An example PMT which shows promising attributes is the Hamamatsu H7422 series detector [181]. The specifications are listed in Table 7.2 and its dimensions can be seen in Figure 7.10. The H7422P-40 and H7422P-50 are appealing as they are small enough to fit in the available space in the payload, are designed specifically for single photon detection, and have internal high-voltage power supply circuits allowing them to run off the limited voltage supply from the satellite system. The 5 mm (diameter) active area allows for a larger field of view from the free space detection and relaxes the constraints on the optics. The typical dark count rate for this device is around 100 cps with a quoted max of 300 cps. This will have to be confirmed for a radiation-filled environment.

The weight of one module is 400 g, so these devices will add 1.6 kg to the payload mass. The max power consumption can be calculated as $18\,\text{V} \times 62\,\text{mA} = 1.12\,\text{W}$. Although the specifications of this device do not exactly agree with the proposed requirements from Table 7.1, for an off-the-shelf unit it comes very close and could still allow for success in this mission with possible modifications.

Parameter	H7422-40	H7422-50
Spectral Response	300 nm to 720 nm	380 nm to 890 nm
Input Voltage	+11.5 V to +15.5 V	+11.5 V to +15.5 V
Effective Area (diameter)	5 mm	5 mm
Peak Sensitivity Wavelength	580 nm	800 nm
Quantum Efficiency at Peak Wavelength	40%	12%

Table 7.2: Detector parameters for the H7422P-40 and H7522P-50 photomultiplier tubes.

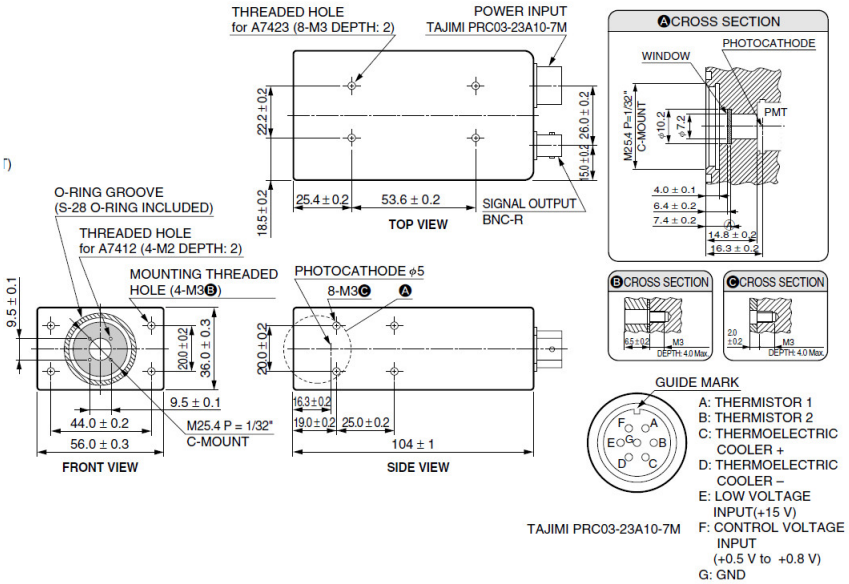
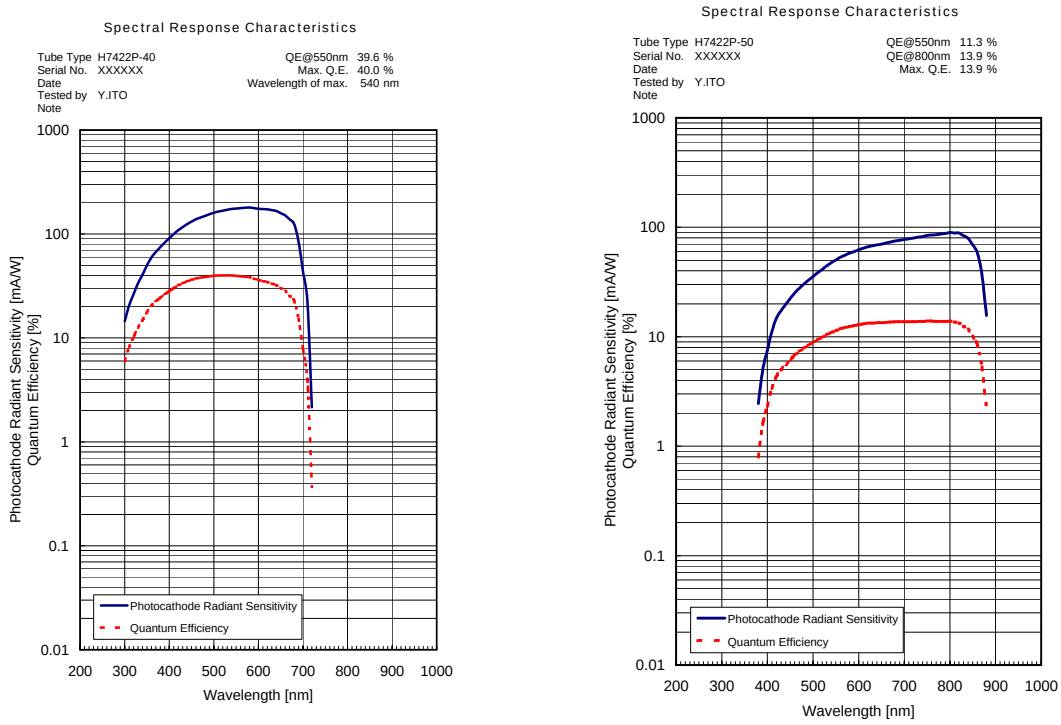


Figure 7.10: Dimensions of the H7422 series detector from the H7422P-40 data sheet [181].



(a) (b)

Figure 7.11: Photocathode sensitivity and quantum efficiency as a function of wavelength for the Hamamatsu (a) H7422P-40 and (b)H7422P-50. From correspondence with Hamamatsu.

One of the drawbacks with these PMTs is that they are more sensitive in the visible wavelength region, which suffers from higher losses during atmospheric transmission. Figure 7.11 shows the detector photocathode sensitivity as well as the quantum efficiency as a function of wavelength of the two models described above.

Ideally, we would choose the wavelength with the highest quantum efficiency for this application, but we must also consider atmospheric transmission. The detector quantum efficiency is above 30% for the wavelengths between about 400 nm and 650 nm for the H7422P-40. At 20% this extends from 350 nm to 685 nm.

The atmospheric transmission must also be taken into account when determining an appropriate signal wavelength. MODTRAN [182], used in this study, is a program which has been developed to model transmission of light propagating through the atmosphere,

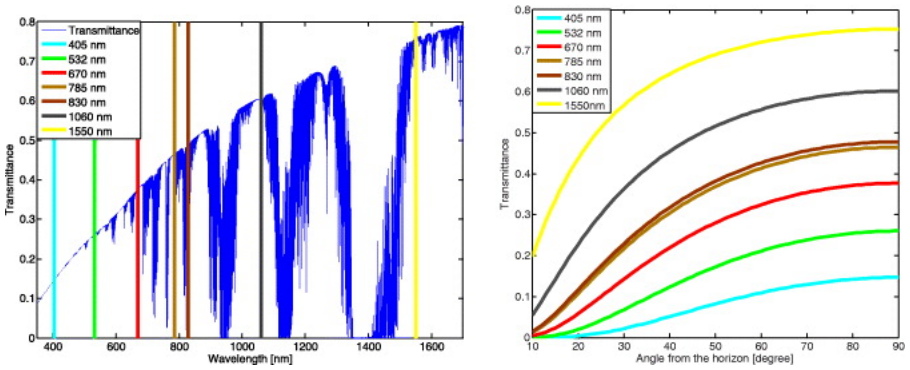


Figure 7.12: Optical transmission through the Earth's atmosphere with common wavelengths highlighted [89].

although there are others [183]. Figure 7.12 shows transmission as a function of wavelength, as generated by MODTRAN, overlaid with commonly used transmission wavelengths.

After comparing the quantum efficiency of the detector to the atmospheric transmission data, we have selected a wavelength of 639 nm. This allows for an atmospheric transmission of 34.5% and a quantum efficiency of 32%. Another benefit of using this wavelength is the availability of laser sources, making the source easier to build. This wavelength is less than that determined by previous studies to be ideal (785 nm), but here we are limited by the choice of detector.

It would be impractical to use these detectors as they are packaged off the shelf with our cooling scheme. Modifications would include removing the PMT module from the casing, allowing it to be cooled separately. The electronics board for the PMT will then be placed elsewhere and kept at the appropriate operating temperature. Furthermore, due to the high voltage required by the PMT, we would need to design appropriate wiring between the electronics board and the PMT.

7.2.2.1 Radiative Cooling

Cooling of the detectors on the satellite can be accomplished in two ways: passive cooling with a radiator, or active cooling with a cooling unit. Passive cooling through a radiator will be the main focus of this study as it reduces both the mass and the power consumption of the satellite. The thermal radiator analysis for this project was done in discussion with UTIAS SFL [152, 184]. Only the final results will be presented here.

The main goal is to find a relation between the size of the radiator, and its potential

Variable	Value	Definition	Source
A	[m^2]	Area of the radiator	
Q_1	$Q + Q_{L1}$	Heat transfer between the detectors and the radiator	[184]
Q	4 W/m^2	Heat dissipation of the detectors	[181]
Q_{L1}	$\frac{T_{sat}-T_{obj}}{R_1}$	Heat leakage from the satellite to the detectors	[184]
T_{sat}	293.15 K	Average temperature of the satellite body	Estimate
T_{obj}	278.15 K	Desired temperature of the detectors	Estimate
R_1	10 K·m^2/W	Heat resistance between the detector and the satellite	Estimate
ϵ	0.75	Emissivity of the radiator	[152]
σ	5.67051×10^{-8} W/m^2/K^4	Stephan-Boltzmann Constant	[152]
T_{det}	[K]	Final temperature of the detectors	
R_{COND}	10 K·m^2/W	Heat resistance between the detectors and the radiator	Estimate
Q_{L2}	0 W/m^2	Heat leakage from the satellite to the radiator	Approximation
Q_A	$F\alpha a Q_{solar}$	Heat flux from albedo of the Earth	[184]
F	0.249	View factor of the radiator to the Earth	[184]
a	0.23	Average albedo	[152]
α	0.13	Average solar absorptance of aluminum	[152]
Q_{solar}	1367 W/m^2	Average solar heat flux	[152]
Q_{IR}	$F\epsilon Q_{E,IR}$	Earth infrared heat flux	[184]
$Q_{E,IR}$	231 W/m^2	Average Earth infrared heat flux	[152]

Table 7.3: List of the parameters used to calculate the temperature response of the detectors based on the size of the radiator

to cool the detectors. Reference [184] has given this relation as:

$$A \geq \frac{Q_1}{\epsilon\sigma(T_{\text{det}} - Q_1 R_{\text{COND}})^4 - Q_{L2} - Q_A - Q_{IR}}, \tag{7.1}$$

where the variables are defined in Table 7.3. As a very simple approximation, it is assumed that there is no heat leakage from the satellite body to the radiator, although this will certainly need to be studied further. To make the results a little more practical, Equation 7.1 is reworked in terms of length of one side of the radiator rather then the area (assuming a square radiator), and is also explicitly solved for the temperature instead of the size. The new equation becomes

$$T_{\text{det}} = Q_1 R_{\text{COND}} + \frac{(S^2(Q_1 + (Q_A + Q_{IR})S^2)\epsilon\sigma)^{\frac{1}{4}}}{S\sqrt{\epsilon\sigma}}, \tag{7.2}$$

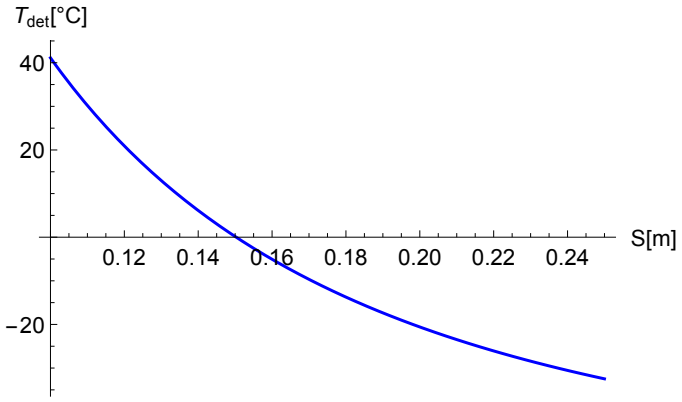


Figure 7.13: The temperature of the detectors decreases as the length of one side of the radiator increases (assuming a square radiator). This simple estimate demonstrates that a radiator of approximately 15 cm×15 cm would cool the detectors to approximately 0 °C.

where S is the length of one side of the radiator. Figure 7.13 shows a plot of the detector temperature in °C as a function of the length of one side of the radiator.

From the analysis, it can be seen that the detectors can be cooled to approximately 0 °C with a square radiator with side length 15 cm. This matches well with the location where the radiator is mounted to the payload. Two of the detectors are mounted close to the radiator and two are on the opposite side. This will create a slight temperature difference between the detectors on one side as opposed to the other. A clever heat pipe system will need to be designed to minimize this separation so the detectors can work at approximately equal temperatures.

7.2.3 Data Processing

Previous studies have shown a 1GHz ARM processor is sufficient for the expected performance and functional requirements of the QEYSSAT mission. A design has been proposed which will make use of of a processor module plus a daughter board. This has the advantage of using space-qualified processor module while having the flexibility to adapt the daughter board to the specific needs of QKD. Figure 7.14 shows a diagrammatic scheme of the processing system.

The processor module will be a commercial off–the–shelf device and will most likely be based on a Xilinx ZYNQ device. This module offers the following features:

- FPGA implementation for time-tagging for the prototype processor board

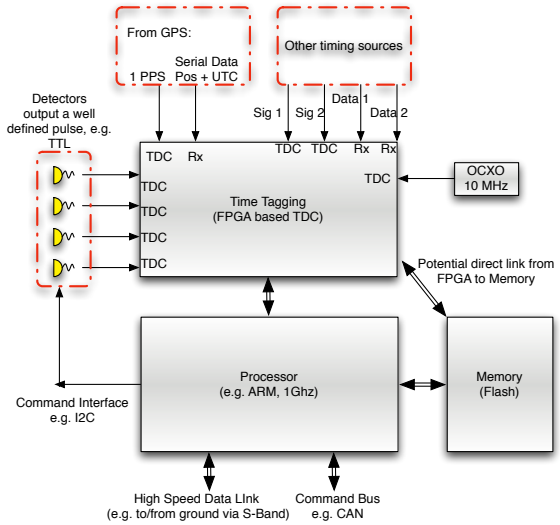


Figure 7.14: Functional schematic diagram for the processor board and timing hardware as proposed for QEYSSat from QKDR Proposal - Section I - Technical-Management (2013)

- FPGA logic for OBC connection (if required)
- Central processing unit (CPU) and random access memory (RAM)
- Mass storage

The daughter board as proposed for QEYSSAT will be reduced in size and will include:

- Connection to DAQ board
- Connection to the notional spacecraft OBC and power subsystem interface
- Specialized OCXO required for precise time-tagging
- Power conditioning (if required)
- Connection to the processor module

Parameter	Value
Time-tag unit/precision	78 ps
Time register width	34 bits
Channel register width	3 bits
Total bits per time-tag	37 bits
Total with byte alignment	40 bits
Duration of measurement	300 s
Maximum received average time-tag rate	100 kHz
Time to stream 100k tags (2Mbit link)	2 s
Time to stream 100k tags (5Mbit link)	0.8 s
Time to stream 5min worth of tags (2Mbit)	600 s
Time to stream 5min worth of tags (5Mbit)	240 s

Table 7.4: Communication requirements for the transmission of the raw tags from the satellite to the ground as studied in Canadian Quantum Communication Satellite: Concepts and Components (2012).

For initial investigations into a processor board we considered a ZedBoard (Xilinx: Zynq-7000 All Programmable SoC) [185]. Many of the budget characteristics such as power and mass were based off those of this board. Table 7.4 demonstrates the classical communication requirements of the system as described by a study conducted for QEYSSAT.

7.2.4 Payload Assembly

Figure 7.15 shows a 3D rendering of the payload volume with components installed. The large circular aperture in the front is filled with the primary telescope lens. The processing and electronics boards are also located in the large front portion of the volume. The back, smaller portion of the volume contains the polarization analyzer and the detectors. Currently the detectors are placed in with their default packaging, but this can be changed to reduce the space they use. The radiator can be seen on the side of the satellite and will be used to cool the detectors.

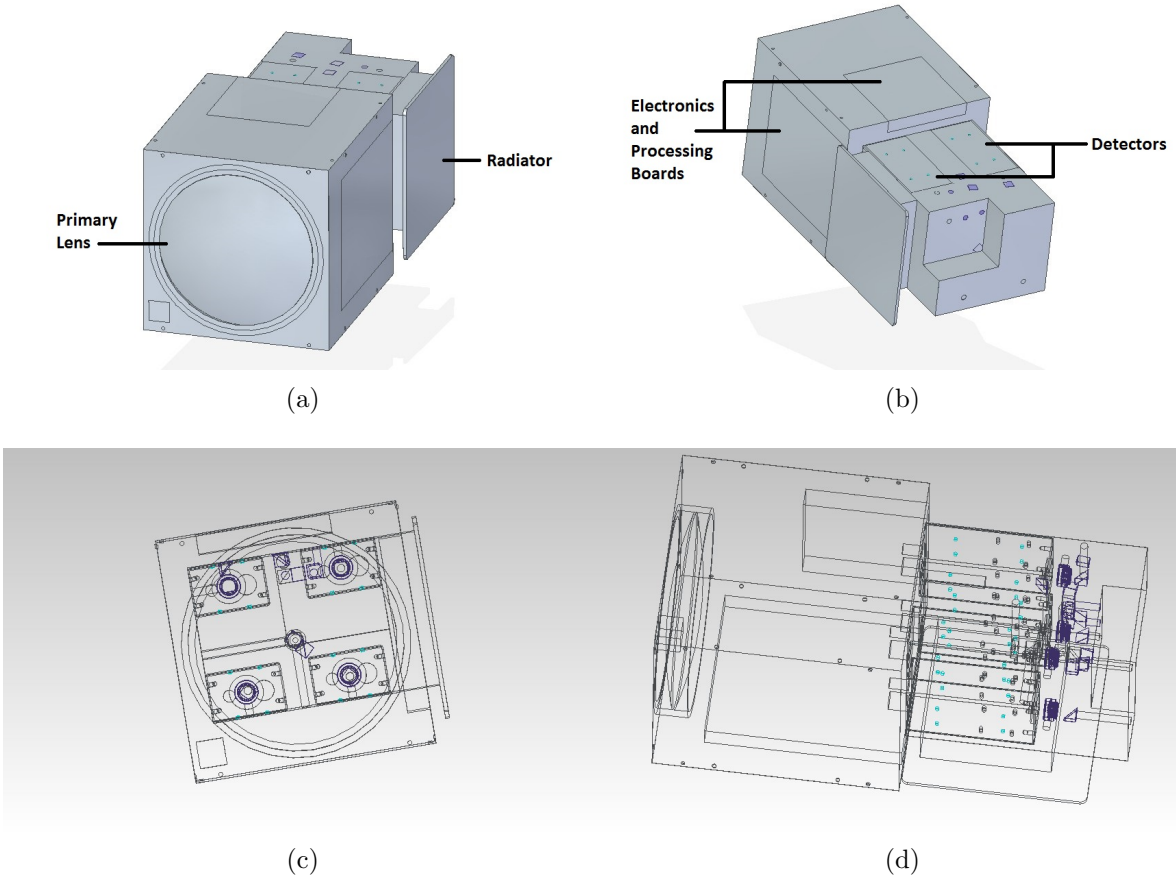


Figure 7.15: (a) Solid model of the payload enclosure from the front. The large primary lens can be seen here as well as the radiator at the rear-right of the diagram. (b) Rear view of the payload enclosure. The electronics and processing boards can be seen in the rear portion of the image, and the detectors can be seen in the forward portion. (c) Wire model of the payload volume viewing from the front. The detectors are facing towards the rear in this view. (d) A side wire model of the payload volume with the detectors and optics placed inside. The square boxes in the large box in the front of the volume are the electronics and processing boards.

7.3 Pointing and Ground Station Location

One of the main advantages of NanoQEY is that there is no fine pointing system on the satellite. However, because of this, a wider field of view as well as good course pointing from the satellite are required. One scheme that was studied is the idea of constant rate tracking as this would simplify the coarse pointing of the satellite towards the ground station.

It would also be beneficial for the payload software to access data directly from the star tracker to add to the time-tagger data. This will allow us to remove sections of data in post-processing where the satellite is known to have not been in proper alignment and hopefully increasing the length of secure key.

7.3.1 Constant Rate Tracking

Constant rate tracking has the satellite performing a constant rotation as it flies over the ground station. This will be implemented by the satellite with reaction wheels. The satellite will not actively track the ground station, but will instead have it come in and out of view as the satellite rotates overhead.

Initial analysis of the constant rate tracking demonstrated positive results, but only incorporated one dimension of rotation. This means that one rotation axis of the satellite will be fixed on a specific target, but the other will be constantly rotating. After including the second axis of rotation it appears constant rate tracking is no longer be feasible. The field of view for this analysis was asymmetric and given by a 0.4° field of view in one dimension and 0.1° field of view in the other dimension. The smaller field of view in one dimension is possible because the satellite will only be changing pointing in one direction and therefore have the ground station always in view from the perspective of the other direction. Figure 7.16 demonstrates a best pass, upper-quartile pass and median pass, in terms of link time and approach near zenith, with this tracking scheme.

The best pass of the satellite actually performs very poorly with this pointing scheme and the upper-quartile pass has the longest contact time. This analysis shows that NanoQEY will require target tracking which will increase the strain on the pointing requirements of the satellite. The satellite is capable of target tracking using both a star tracker as well as reaction wheels, but it was hoped that constant rate target tracking would simplify the tracking requirements. By using target tracking, the asymmetric field of view can be removed thus simplifying the required optics.

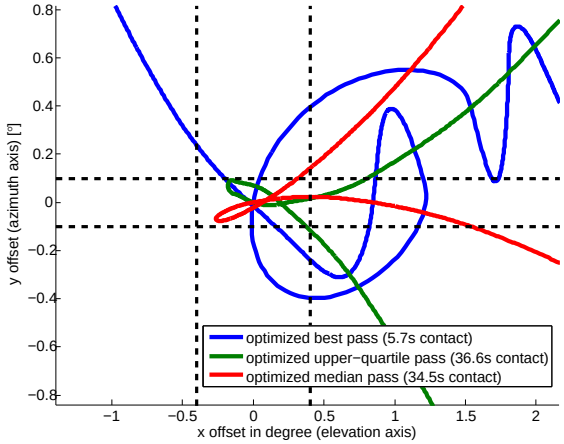


Figure 7.16: Performance of constant rate tracking optimized in elevation and azimuthal angles. Constant rate tracking performs quite poorly for the best pass (blue) as it only has 5.7 s of contact time. The longest link duration was 36.6 s in the upper-quartile pass (green), but was still very short and not feasible for effective key generation.

7.3.2 Beacon Laser

NanoQEY uses a beacon laser which will assist the ground station in tracking the satellite. The beacon laser will have a wavelength around 810 nm. Part of this study was to determine the power received by a collector $1\,\mathrm{m}^2$ in area based on the initial power of the beacon laser. Figure 7.17 shows the satellite above the Earth emitting the beacon laser with a field of view of 0.4 degrees and orbiting at 600 km.

The photon flux is dependent on the wavelength and can be calculated by

$$\Phi(P, \lambda) = \frac{P\lambda}{hc}, \tag{7.3}$$

where P is the initial power of the beacon laser, h is Plank's constant, c is the speed of light, and λ is the wavelength of the beacon laser. In order to find the power at the ground site per square meter, we must calculate the photon flux divided by the area covered by the beam (only considering diffraction)

$$P = \frac{\Phi}{A} \times \frac{hc}{\lambda}, \tag{7.4}$$

where A is the diffraction limited area on the ground. With this simple model, the received power at a $1\,\mathrm{m}^2$ receiver can be seen in Figure 7.18.

Since the difficulty of receiving this low power ($\sim 10\,\mathrm{nW}$) will be at the ground station, we will assume that it can be done with proper filtering as well as good detectors. For the

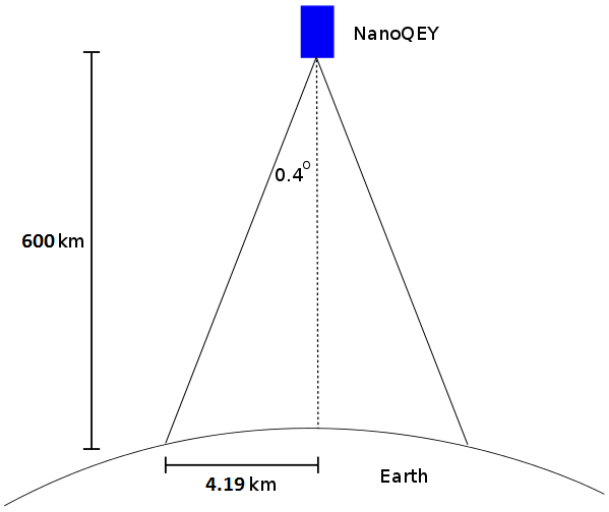


Figure 7.17: Beacon laser field of view on ground for power analysis.

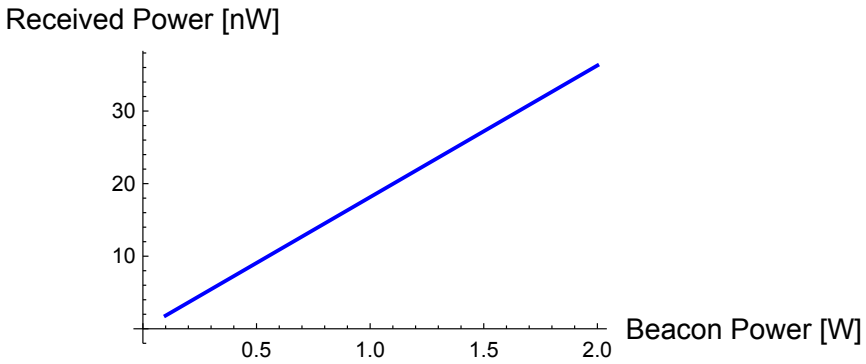


Figure 7.18: Power at a one square meter receiver as a function of the output power of the beacon laser. Even with a 1 W beacon laser, the ground station will only register ~ 10 nW of power, and this is only due to the geometrical effects.

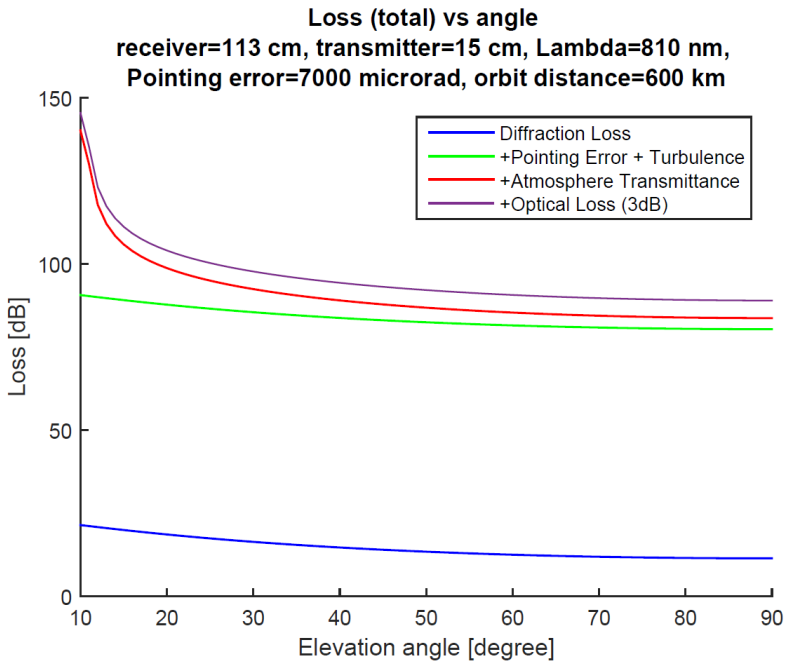


Figure 7.19: Loss budget for beacon laser including atmospheric loss as well as other aspects, versus elevation angle. In this case, the receiver diameter is 113 cm (giving an effective area of 1 m^2), the transmitter is 15 cm in diameter, the wavelength is 810 nm and the pointing error is 7 mrad.

power budget, we will assume a 1 W diode laser at 810 nm. The loss just from the simple calculation is around 80 dB, which can be considered the best case scenario. Investigating a little further and making a few more assumptions about the beacon laser, we modeled the transmission loss from the satellite to the ground including atmospheric loss etc. This can be seen in Figure 7.19.

With this new analysis, it can be seen that instead of having around 80 dB of loss, it will be closer to 95 dB to 100 dB which, if given an initial power of 1 W, would lead to 100 pW, at the detector. Again, because this is at the ground station, this is still possible.

7.3.3 Location

In a previous study [89], background emissions were analyzed from various locations around 45 km from Ottawa. These locations where chosen to demonstrate the concept of a ground station that could extend the range of local city wide QKD network, thus linking cities using satellites. These sites were shown to be suitable for a satellite QKD up-link when fine pointing is used to achieve $<50\,\mu$rad pointing error. Coarse pointing of the satellite

is estimated to only provide on the order of 0.4° (7 mrad) pointing accuracy, requiring an equally large field of view. Figure 7.20 shows the observed area, and its corresponding background contribution, for a location 45 km from Ottawa. The background is almost entirely due to the artificial light from sources surrounding the ground station. This amount of background would be far too much for a successful QKD link and therefore renders this site as unusable.

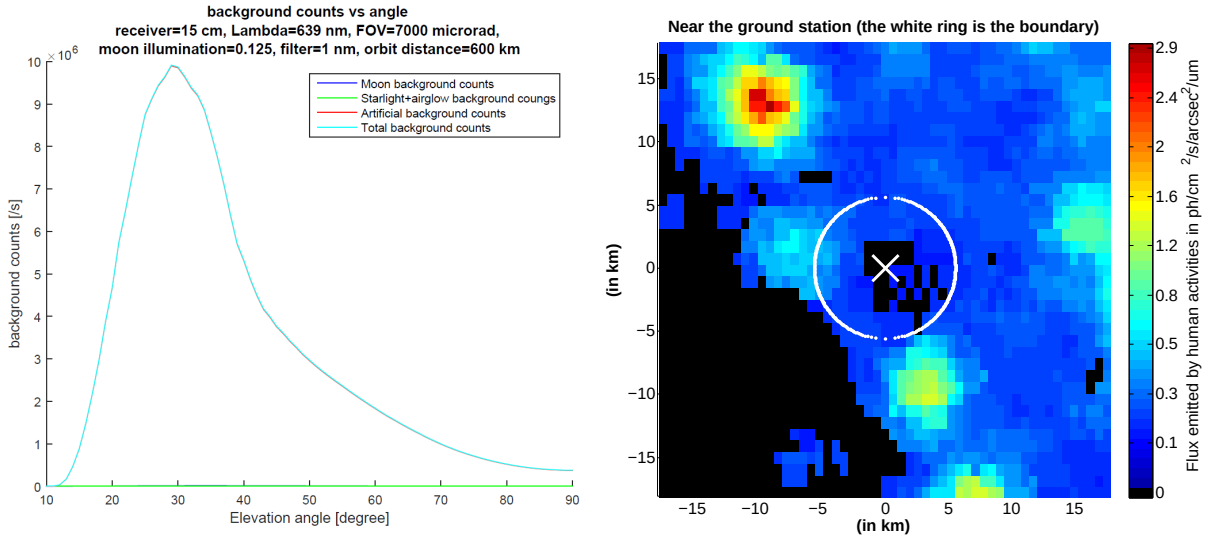


Figure 7.20: Background light contributions 45 km from Ottawa with 0.4° field of view. Artificial light from surrounding sources produces on the order of 10 million photons per second. The moon is assumed to be reflecting the sun from $\frac{1}{8}$ of its area, wavelength is 639 nm, receiver is 15 cm, filter is 1 nm. The atmosphere is assumed to be rural sea-level and the orbit altitude is 600 km.

Two new locations were considered to assess the feasibility of satellite QKD without fine pointing. The first is mount Teide on Tenerife, the largest island of the Canary Islands. Tenerife offers a good atmospheric location with an astronomical observatory 2.35 km above sea level that has been previously used for ground demonstrations of QKD. The area on the mountain is almost completely free of light pollution. However, the area surrounding it has high levels of artificial background captured by the field of view when the satellite is at lower elevation angles (see Figure 7.21), causing background counts on the order of a million photons per second.

The second location considered is in Algonquin Provincial Park. This location does not offer the high elevation of Tenerife, and thus will not offer as good atmospheric conditions. However, the park has almost no light pollution, while being located in southern Ontario and thus easily accessible. In this location, the background is dominated almost exclusively

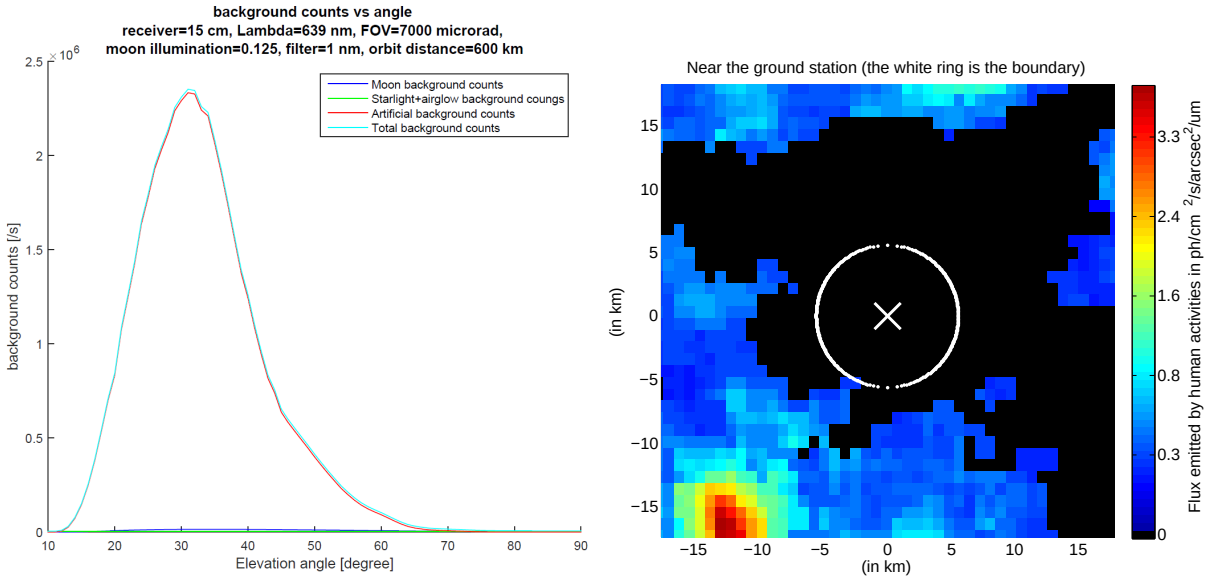


Figure 7.21: Background light contributions at Tenerife with 0.4° field of view. Light pollution surrounding the mountain is captured when the satellite is at lower elevations. The moon is assumed to be reflecting the sun from $\frac{1}{8}$ of its area, wavelength is 639 nm, receiver is 15 cm, filter is 1 nm. The atmosphere is assumed to be rural sea-level and the orbit altitude is 600 km.

by the moon, starlight and airglow as shown in Figure 7.22).

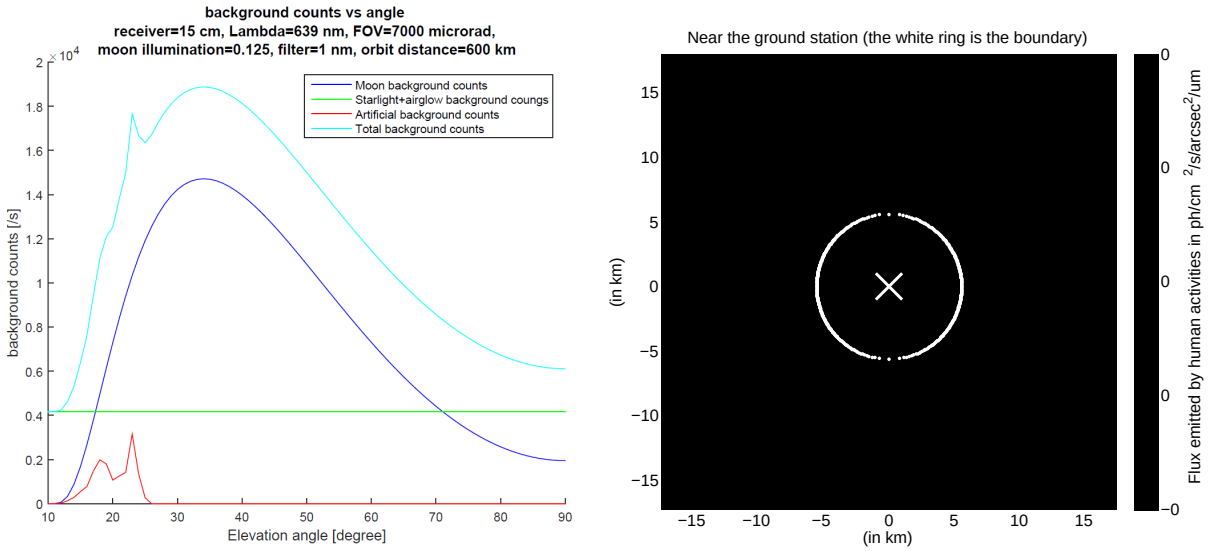


Figure 7.22: Background light contributions at Algonquin park with 0.4° field of view. This location offers a very low artificial background contribution. The moon is assumed to be reflecting the sun from $\frac{1}{8}$ of its area, wavelength is 639 nm, receiver is 15 cm, filter is 1 nm. The atmosphere is assumed to be rural sea-level and the orbit altitude is 600 km.

7.4 Predicted Performance

The link analysis (using the methods of [89]) showed that the system can only perform well in a location with very low artificial background and on nights with no moon visible in the sky. The moon background contribution significantly hinders the performance of the system. Even with a 0.1 nm filter, having $\frac{1}{8}$ of the moon illuminated is sufficient to reduce the amount of key generated by an order of magnitude compared to a 1 nm filter with no moon.

When no moon is present, the background is sufficiently low for the performance to be almost unaffected by a narrower filter. Using a 0.1 nm filter, compared with a 1 nm filter, produced similar results, with less than 6% difference in performance. It seems that having a narrower filter is unnecessary when using a very good location with no moon, and is insufficient in less ideal locations or during nights where the moon is visible. This method should be considered if the location used has a smaller area of very low artificial background as well as possibly reducing the field of view. For example, the observatory on the island of Tenerife has low artificial background for an approximately 5 km radius, which is insufficient for a 0.4° field of view, but may perform well with a 0.2° field of view.

Tables 7.5 and 7.6 show the predicted performance for the planned system. Due to the

	Secure key [Mbit/month]		
Detector dark [cps]	**WCP source, sea-level**	**WCP source, mountain**	**Entangled photon source, mountain**
20	0.112	1.259	0.052
100	0.011	0.870	0.043
300	0	0.303	0.026
1000	0	0	0.0002

Table 7.5: Predicted key generation performance. 639 nm wavelength, 50 cm ground transmitter, 15 cm satellite receiver, 600 km orbit, 2 μrad pointing error of the ground station, 0.4° satellite field of view. Rural atmosphere (5 km visibility) with no moon and similar artificial light as Algonquin park, assuming a 50% chance of cloud cover. WCP source rate of 300 MHz, entangled photon source rate of 100 MHz, 0.5 ns detection time window, 1 nm filter bandpass. Although Algonquin park provides a very nice site, access to this location could prevent its use. This shows the feasibility of generating key with NanoQEY

small impact of the narrower filter, only results with 1 nm filter are shown. The entangled photon source at sea-level is not shown because it was not able to produce key. Mountain location is 2.3 km above sea-level.

	Usable passes [/month]		
Detector dark [cps]	**WCP source, sea-level**	**WCP source, mountain**	**Entangled photon source, mountain**
20	7.500	15.000	8.958
100	2.792	12.333	7.792
300	0	7.042	6.208
1000	0	0	0.167

Table 7.6: Predicted number of usable passes per month. 639 nm wavelength, 50 cm ground transmitter, 15 cm satellite receiver, 600 km orbit, 2 μrad pointing error of the ground station, 0.4° satellite field of view. Rural atmosphere (5 km visibility) with no moon and similar artificial light as Algonquin park, assuming a 50% chance of cloud cover. WCP source rate of 300 MHz, entangled photon source rate of 100 MHz, 0.5 ns detection time window, 1 nm filter bandpass.

7.5 Engineering Budgets

In order to determine if the components which have been studied in the previous sections are feasible with the proposed satellite bus, we will now analyze the power and mass of the components. The satellite offers the payload a total of 5.1 Whr per pass to operate. The mass constraint for the payload (including the enclosure housing) is 7.5 kg.

Table 7.7 demonstrates a typical pass of the satellite over the ground station and the power consumed at each stage. The equipment will need to initialize and thermalize before the ground station is actually in sight. Once all the systems are on and ready, the ground station will come into sight and QKD can begin. Once the pass is complete, post processing will occur and the satellite will have to transfer the results to the ground station.

Tables 7.8 and 7.9 show the mass estimates of each of the components as proposed above. A margin is calculated for each mass as well as a 10% contingency. Many of these components are just example components and will need to be further studied for space compatibility. Table 7.9 shows a ≈900 g overage in mass, but this is possible to scale back by clever choice of the housing material.

Task	Task Duration [s]	Task Start/End	Processor Board	Detectors	Beacon Laser	Total Power [W]	Energy [Whr]
Initialization of processor board	1	00:00:01 00:00:02	15.6	0	0	15.6	0.00433
Idle before detectors on	60	00:00:02 00:01:02	2.6	0	0	2.6	0.04767
Initialization of detectors	1	00:01:02 00:01:03	2.6	3.8688	0	6.4688	0.04946
Idle before data collection	300	00:01:03 00:01:08	2.6	3.8688	0	6.4688	0.58853
Beacon laser turns on	10	00:01:08 00:01:18	2.6	3.8688	5	11.4688	0.62039
Data collection and link acquisition	300	00:01:18 00:06:18	3*	3.8688	5	11.8688	1.60945
Post processing	60	00:06:18 00:07:18	3*	0	0	3	1.65945
Idle post operation	0	00:07:18 00:07:18	3*	0	0	3	1.65945
Data transfer	300	00:07:18 00:12:18	2.6	0	0	2.6	1.87612
*best estimate						Peak Power = 15.6 W	Energy Used = 1.876 12 Whr

Table 7.7: Power estimates for the various components in the payload.

System	Component	CBE [kg]	Margin [%]	Cont. [%]	Total [kg]	Basis of Estimate
Optics	5 Filters	0.136	10%	10%	0.163	Thorlabs Bandpass Filters
	Telescope	0.700	15%	10%	0.875	IQC analysis (C. Pugh, C. Holloway, 10/29/2013)
	5 Beam Splitters	0.136	10%	10%	0.163	Thorlabs 4xPBS 101 and 1x BS010
	9 Mirrors	0.245	10%	10%	0.294	Thorlabs 9xBB05-E02-1/2
	Optical Bench and Support/ Mounting Assemblies	0.350	20%	10%	0.455	Thorlabs Mini Series Mounting Posts (∼15) Large Lens Mount
	5 Focusing Lenses	0.113	10%	10%	0.136	Thorlabs LA4647
	Retroreflector	0.113	10%	10%	0.136	Thorlabs PS975M
	Dichroic Beam Splitter	0.050	20%	10%	0.026	Thorlabs DMLP505T
Detector	PMT	1.600*	10%	10%	1.920	Hamamatsu H7422 Spec Sheet
	Thermal Plate and copper braiding	0.300†	20%	10%	0.390	Estimate
	Mechanical Structure and Supports	0.050	20%	10%	0.065	Just screws if casing is used
Board	DAQ Processor and Board	0.150	20%	10%	0.195	Estimate by lifting a sample
	Input Power Filter	0.100	20%	10%	0.130	Estimate by lifting example (*includes plastic)
	A/D Converter	0.100	20%	10%	0.130	Estimate
	Mechanical Structure and Supports	0.100	20%	10%	0.130	Estimate
Other	Receiver Enclosure/Housing	1.700††	15%	10%	2.125	Calculation assuming Aluminum and 0.25cm thickness
	Radiator Panel and Support Structure	0.270	15%	10%	0.338	$15 \times 15 \times 0.3$cm Aluminum and estimated support structure (100cm^3)
	DC Power Supply Board	0.100	20%	10%	0.130	Estimate
	Fasteners	0.100	20%	10%	0.130	Estimate
	Power Cables and Connectors	0.100	20%	10%	0.130	Estimate
	Data Cables and Connectors	0.050	20%	10%	0.065	Estimate
	Beacon Laser	0.194	15%	10%	0.242	PicoLAS Spec Sheet

* will be lowered with removal of factory casing.

† will depend on PMT mounting method.

†† can be reduced with an optimized structure.

Table 7.8: Mass estimates for the NanoQEY payload.

Current Best Estimate (CBE) Mass Total [kg]:	8.368
Allowable Mass Requirement [kg]:	7.500
Margin [kg]:	-0.868
Margin [%]:	-11.6%

Table 7.9: Mass totals for the QKD payload of NanoQEY. The mass (including margin) exceeds the allowable budget by 11.6 % but this can be reduced with clever repackaging of the detectors as well as a review into the payload enclosure.

7.6 Schedule

As this mission would utilize the pre-existing UTIAS/SFL nano satellite design, the cost and time line can be reduced. Using the "microspace" approach from UTIAS/SFL the project could feasibly be developed in 2.5 years from project kick-off followed by a 1 year operational period. A predicted schedule can be seen in Figure 7.23.

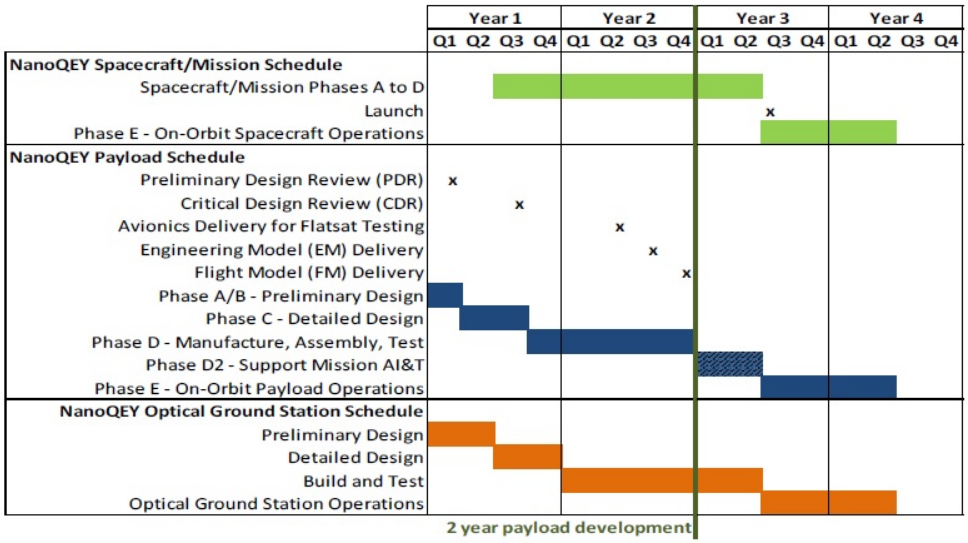


Figure 7.23: A predicted time line for the NanoQEY mission. The satellite could be designed and built in 2.5 years from project start and then be followed by a 1 year orbit period.

7.7 Discussion

In order to implement the wide field of view required by removing the fine pointing system, a few trade-offs are required. First of all, the restrictions on the ground station have been increased. Since the effective area the satellite sees on the ground is larger than with a system that implements fine pointing, the site must have far less background light. This restricts the ground station from being near cities as they generate too much light pollution. Very narrow-band filters (<1 nm) were investigated but seem to show no impact on the performance.

The nano satellite also provides a larger restriction on the mass, volume and power constraints of the system. With clever engineering and appropriate device selection, these requirements can be met to fit in the 7.5 kg mass budget and the given volume budget.

Utilizing a radiator for cooling the detectors will simplify the satellite by not requiring cooling units which contribute to the mass, volume, and power budgets, as well as reduce available space for other components. The study shows that a radiator of sufficient size will fit on the satellite and will be effective as long as an effective heat dissipation method is developed for the interior of the satellite.

The constant rate tracking algorithm was explored and deemed not usable for this mission. The satellite will require target tracking mechanisms such as a star tracker in

order for the mission to be successful.

7.8 Conclusion

We performed a study, along with UTIAS SFL, to determine the feasibility of building a nano satellite using the existing NEMO bus with a compact QKD receiver payload to perform QKD between the Earth and a satellite. It was determined that this concept is feasible and practical with current technology. The study identified potential components to investigate further for implementation into the NanoQEY mission. Although the requirements on the ground station are stricter with this mission, this portion of the mission is not the focus of this study as we only consider the space portion.

Chapter 8

Conclusion and Outlook

In order to eventually move towards global quantum cryptography, the distance problem of transmitting quantum secured keys between two locations further than a few hundred kilometers must be solved. Although fibers provide convenient media to transmit the photons on a local level, they currently are not feasible for global schemes. This is where satellite QKD will thrive and be able to connect stations around the world.

In this thesis, a variety of topics were studied and demonstrated to show work towards this ultimate goal of satellite QKD. In Chapter 2 a theoretical study into the feasibility of using adaptive optics to help solve the problem of the large loss when performing an optical up-link to a satellite was studied. The anisoplanatism term dominates this error, but techniques to mitigate this term were proposed. The results are promising, but of course, polarization effects must be taken into account when manipulating the quantum signal. It is also very important to study the atmospheric conditions of the chosen ground station locations as this is a huge factor in the loss for a given up-link geostationary orbits were also studied and although the geometric loss is larger due to the greater distance, the anisoplanatism error is no longer the dominant term. The system bandwidth becomes a greater issue which can be solved through development of better and faster devices.

In order to maximize the number of photons collected, it is important for fine pointing systems to be implemented. Chapter 3 demonstrates the study, design and implementation of a fine pointing unit for a receiver payload to implement QKD. The requirements for this device were derived from practical realities one will face when performing and optical up-link to a satellite. Polarization effects were taken into account and mitigated and a system was designed with a clear path to flight for the potential integration onto a future satellite payload.

Chapters 4 through 6 show a successful demonstration of a prototype quantum key

distribution payload. The core components, consisting of the fine pointing unit, the integrated optical assembly, the detectors, and the control and data processing unit were built with space flight in mind and have a clear path to flight for a satellite implementation. The experiment demonstrated the viability of the up-link scenario for a QKD mission. Until now this had only been theoretically studied but this demonstration gives further evidence to the successful completion of such a mission.

The airborne demonstration pulled together a large team and introduced us to many challenges not normally experienced in a laboratory environment. It also was representative of the operations of a fully functional ground station and the procedures required to successfully complete QKD from a ground station to a moving satellite. The large collaboration also allowed us to improve our abilities in project management and multi-partner collaboration. Many of the risk mitigation strategies that were put in place were crucial for the success of the final experiment.

The NanoQEY proposed mission presented in Chapter 7 demonstrates the feasibility of a nano-satellite which could be used for demonstration of the QKD protocol in an up-link configuration to a satellite. The idea behind this mission proposal is to provide a cost effective, simple, and quick satellite which could be used to demonstrate the feasibility of this technology and protocol. The study looked at the theoretical performance of such a satellite and found some candidate technologies which could be studied further for implementation.

Performing quantum key distribution with satellites has the benefit of helping increase the distance to which QKD can be achieved. By solving this problem, it will allow us to connect any two points around the world with quantum secure information keys. These satellites will help form a global quantum secure network for future data transfers. By incorporating QKD into already existing metropolitan networks, we can generate keys in cities via fiber, and connect cities with satellites. All of this will eventually lead to the *Quantum Internet*. The next steps to move towards this are to implement QKD onto existing fiber networks alongside classical channels, and to continue developing satellites to perform the protocol. Having networks of these satellites will allow for large key rates for each location helping to also solve the current rate problems.

Overall the prospect for quantum communications using satellites is very exciting and governments around the world are becoming very interested in this technology. As mentioned, China has already launched a quantum demonstration satellite and as recent as April 2017, Canada has also expressed intent in a quantum satellite through a funding

announcement with the Canadian Space Agency[3]. The work presented here, along with years of study and development, will provide a great technological and scientific baseline for such a satellite mission for Canada.

[3]Ministers Bains and Garneau celebrate $80.9 million for the Canadian Space Agency. https://www.canada.ca/en/innovation-science-economic-development/news/2017/04/ministers_bains_andgarneaucelebrate809millionforthecanadianspace.html

References

[1] R. Loudon. *The quantum theory of light*. Oxford science publications. Clarendon Press, 1983.

[2] C. Gerry and P. L. Knight. *Introductory Quantum Optics*. Cambridge University Press, 2005.

[3] K. J. Resch. *Quantum Optics Course Notes*. University of Waterloo, 2012.

[4] R. G. Gallager. Low-density parity-check codes, 1963.

[5] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, New York, NY, USA, 10th edition, 2011.

[6] I. Marcikic, H. de Riedmatten, W. Tittel, H. Zbinden, and N. Gisin. Long-distance teleportation of qubits at telecommunication wavelengths. *Nature*, 421(6922):509–513, Jan 2003.

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

[8] A. Mair, A. Vaziri, G. Weihs, and A. Zeilinger. Entanglement of the orbital angular momentum states of photons. *Nature*, 412(6844):313–316, Jul 2001.

[9] I. Bengtsson, G. Adenier, C. A. Fuchs, and A. Y. Khrennikov. Three ways to look at mutually unbiased bases. *AIP Conference Proceedings*, 889(1):40–51, 2007.

[10] G. S. Buller and R. J. Collins. Single-photon generation and detection. *Measurement Science and Technology*, 21(1):012002, 2010.

[11] F. A. Haight. *Handbook of the Poisson distribution*. Publications in operations research. Wiley, 1967.

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

[13] J. Katz and Y. Lindell. *Introduction to Modern Cryptography (Chapman & Hall/Crc Cryptography and Network Security Series)*. Chapman & Hall/CRC, 2007.

[14] C. H. Bennett. Quantum cryptography: Uncertainty in the service of privacy. *Science*, 257(5071):752–753, 1992.

[15] D. Bruß. Optimal eavesdropping in quantum cryptography with six states. *Phys. Rev. Lett.*, 81:3018–3021, Oct 1998.

[16] H. Bechmann-Pasquinucci and N. Gisin. Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography. *Phys. Rev. A*, 59:4238–4248, Jun 1999.

[17] A. K. Ekert. Quantum cryptography based on bell's theorem. *Phys. Rev. Lett.*, 67:661–663, Aug 1991.

[18] E. Biham, M. Boyer, P. O. Boykin, T. Mor, and V. Roychowdhury. A proof of the security of quantum key distribution (extended abstract). In *Proceedings of the Thirty-second Annual ACM Symposium on Theory of Computing*, STOC '00, pages 715–724, New York, NY, USA, 2000. ACM.

[19] D. Mayers. Unconditional security in quantum cryptography. *J. ACM*, 48(3):351–406, May 2001.

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

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

[22] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299(5886):802–803, Oct 1982.

[23] D. Dieks. Communication by epr devices. *Physics Letters A*, 92(6):271 – 272, 1982.

[24] N. Bohr. Das quantenpostulat und die neuere entwicklung der atomistik. *Naturwissenschaften*, 16(15):245–257, 1928.

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

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

[27] H.-Q. Ma, J.-L. Zhao, and L.-A. Wu. Quantum key distribution based on phase encoding and polarization measurement. *Opt. Lett.*, 32(6):698–700, Mar 2007.

[28] K. Inoue and Y. Iwai. Differential-quadrature-phase-shift quantum key distribution. *Phys. Rev. A*, 79:022319, Feb 2009.

[29] M. Bloch, S. W. McLaughlin, J.-M. Merolla, and F. Patois. Frequency-coded quantum key distribution. *Opt. Lett.*, 32(3):301–303, Feb 2007.

[30] M. Mirhosseini, O. S. Magaa-Loaiza, M. N. OSullivan, B. Rodenburg, M. Malik, M. P. J. Lavery, M. J. Padgett, D. J. Gauthier, and R. W. Boyd. High-dimensional quantum cryptography with twisted light. *New Journal of Physics*, 17(3):033033, 2015.

[31] M. Herrero-Collantes and J. C. Garcia-Escartin. Quantum random number generators. *Rev. Mod. Phys.*, 89:015004, Feb 2017.

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

[33] I. Csiszar and J. Korner. Broadcast channels with confidential messages. *IEEE Transactions on Information Theory*, 24(3):339–348, May 1978.

[34] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin. Experimental quantum cryptography. *Journal of Cryptology*, 5(1):3–28, 1992.

[35] G. Brassard and L. Salvail. *Secret-Key Reconciliation by Public Discussion*, pages 410–423. Springer, Berlin, Heidelberg, 1994.

[36] D. J. C. MacKay and R. M. Neal. Near shannon limit performance of low density parity check codes. *Electronics Letters*, 32(18):1645–, Aug 1996.

[37] D. Elkouss, J. Martinez-mateo, and V. Martin. Information reconciliation for quantum key distribution. *Quantum Info. Comput.*, 11(3):226–238, March 2011.

[38] . Mary, M. Gudmundsen, L. Lydersen, and J. Skaar. Error estimation, error correction and verification in quantum key distribution. *IET Information Security*, 8(5):277–282, Sept 2014.

[39] J. L. Carter and M. N. Wegman. Universal classes of hash functions. *Journal of Computer and System Sciences*, 18(2):143 – 154, 1979.

[40] G.S. Vernam. Secret signaling system, July 22 1919. US Patent 1,310,719.

[41] C.-H. F. Fung, X. Ma, and H. F. Chau. Practical issues in quantum-key-distribution postprocessing. *Phys. Rev. A*, 81:012318, Jan 2010.

[42] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill. Security of quantum key distribution with imperfect devices. *Quantum Info. Comput.*, 4(5):325–360, September 2004.

[43] N. Jain, B. Stiller, I. Khan, D. Elser, C. Marquardt, and G. Leuchs. Attacks on practical quantum key distribution systems (and how to prevent them). *Contemporary Physics*, 57(3):366–387, 2016.

[44] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders. Limitations on practical quantum cryptography. *Phys. Rev. Lett.*, 85:1330–1333, Aug 2000.

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

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

[47] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo. Practical decoy state for quantum key distribution. *Phys. Rev. A*, 72:012326, Jul 2005.

[48] Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian. Experimental quantum key distribution with decoy states. *Phys. Rev. Lett.*, 96:070502, Feb 2006.

[49] T. Meyer, H. Kampermann, M. Kleinmann, and D. Bruß. Finite key analysis for symmetric attacks in quantum key distribution. *Phys. Rev. A*, 74:042340, Oct 2006.

[50] M. Hayashi. Upper bounds of eavesdropper's performances in finite-length code with the decoy method. *Phys. Rev. A*, 76:012329, Jul 2007.

[51] V. Scarani and R. Renner. Quantum cryptography with finite resources: Unconditional security bound for discrete-variable protocols with one-way postprocessing. *Phys. Rev. Lett.*, 100:200501, May 2008.

[52] S.-H. Sun, L.-M. Liang, and C.-Z. Li. Decoy state quantum key distribution with finite resources. *Phys. Lett. A*, 373(30):2533 – 2536, 2009.

[53] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden. Quantum key distribution over 67 km with a plug and play system. *New Journal of Physics*, 4(1):41, 2002.

[54] P. A. Hiskett, D. Rosenberg, C. G. Peterson, R. J. Hughes, S. Nam, A. E. Lita, A. J. Miller, and J. E. Nordholt. Long-distance quantum key distribution in optical fibre. *New Journal of Physics*, 8(9):193, 2006.

[55] A. R. Dixon, Z. L. Yuan, J. F. Dynes, A. W. Sharpe, and A. J. Shields. Gigahertz decoy quantum key distribution with 1 mbit/s secure key rate. *Opt. Express*, 16(23):18790–18797, Nov 2008.

[56] 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, Aug 2009.

[57] B. Korzh, C. C. W. Lim, R. Houlmann, N. Gisin, M. J. Li, D. Nolan, B. Sanguinetti, R. Thew, and H. Zbinden. Provably secure and practical quantum key distribution over 307 km of optical fibre. *Nat. Phot.*, 9:163–168, 2015.

[58] A. Poppe, M. Peev, and O. Maurhart. Outline of the secoqc quantum-key-distribution network in vienna. *International Journal of Quantum Information*, 06(02):209–218, 2008.

[59] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, A. W. Sharpe, Z. L. Yuan, A. J. Shields, S. Uchikoga, M. Legré, S. Robyr, P. Trinkler, L. Monat, J.-B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Länger, M. Peev, and A. Zeilinger. Field test of quantum key distribution in the tokyo qkd network. *Opt. Express*, 19(11):10387–10409, May 2011.

[60] R. J. Hughes, J. E. Nordholt, K. P. McCabe, R. T. Newell, C. G. Peterson, and R. D. Somma. Network-centric quantum communications with application to critical infrastructure protection. *CoRR*, abs/1305.0305, 2013.

[61] C. Elliott. Quantum cryptography. *IEEE Security Privacy*, 2(4):57–61, July 2004.

[62] D. Stucki, N. Walenta, F. Vannel, R. T. Thew, N. Gisin, H. Zbinden, S. Gray, C. R. Towery, and S. Ten. High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres. *New J. Phys.*, 11(7):075003, 2009.

[63] Y. Liu, T.-Y. Chen, J. Wang, W.-Q. Cai, X. Wan, L.-K. Chen, J.-H. Wang, S.-B. Liu, H. Liang, L. Yang, C.-Z. Peng, K. Chen, Z.-B. Chen, and J.-W. Pan. Decoy-state quantum key distribution with polarized photons over 200 km. *Opt. Express*, 18(8):8587–8594, Apr 2010.

[64] C. Holloway, E. Meyer-Scott, C. Erven, and T. Jennewein. Quantum entanglement distribution with 810 nm photons through active telecommunication fibers. *Opt. Express*, 19(21):20597–20603, Oct 2011.

[65] N. A. Peters, P. Toliver, T. E. Chapuran, R. J. Runser, S. R. McNown, C. G. Peterson, D. Rosenberg, N. Dallmann, R. J. Hughes, K. P. McCabe, J. E. Nordholt, and K. T. Tyagi. Dense wavelength multiplexing of 1550nm qkd with strong classical channels in reconfigurable networking environments. *New Journal of Physics*, 11(4):045012, 2009.

[66] D. Lancho, J. Martinez, D. Elkouss, M. Soto, and V. Martin. *QKD in Standard Optical Telecommunications Networks*, pages 142–149. Springer Berlin Heidelberg, Berlin, Heidelberg, 2010.

[67] Abdulsalam Ghalib Alkholidi and Khaleel Saeed Altowij. Free space optical communications theory and practices. In Mutamed Khatib, editor, *Contemporary Issues in Wireless Communications*, chapter 05. InTech, Rijeka, 2014.

[68] B. E. A. Saleh and M. C. Teich. *Fundamentals of Photonics*. Wiley Series in Pure and Applied Optics. Wiley, 2007.

[69] W. T. Buttler, R. J. Hughes, P. G. Kwiat, S. K. Lamoreaux, G. G. Luther, G. L. Morgan, J. E. Nordholt, C. G. Peterson, and C. M. Simmons. Practical free-space quantum key distribution over 1 km. *Phys. Rev. Lett.*, 81:3283–3286, Oct 1998.

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

[71] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Omer, M. Furst, 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, Jul 2007.

[72] T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, A. Zeilinger, and H. Weinfurter. Experimental demonstration of free-space decoy-state quantum key distribution over 144 km. *Phys. Rev. Lett.*, 98:010504, Jan 2007.

[73] G. Vallone, V. D'Ambrosio, A. Sponselli, S. Slussarenko, L. Marrucci, F. Sciarrino, and P. Villoresi. Free-space quantum key distribution by rotation-invariant twisted photons. *Phys. Rev. Lett.*, 113:060503, Aug 2014.

[74] S. Nauerth, F. Moll, M. Rau, C. Fuchs, J. Horwath, S. Frick, and H. Weinfurter. Air-to-ground quantum communication. *Nat. Phot.*, 7:382–386, 2013.

[75] J.-Y. Wang, B. Yang, S.-K. Liao, L. Zhang, Q. Shen, X.-F. Hu, J.-C. Wu, S.-J. Yang, H. Jiang, Y.-L. Tang, B. Zhong, H. Liang, W.-Y. Liu, Y.-H. Hu, Y.-M. Huang, B. Qi, J.-G. Ren, G.-S. Pan, J. Yin, J.-J. Jia, Y.-A. Chen, K. Chen, C.-Z. Peng, and J.-W. Pan. Direct and full-scale experimental verifications towards ground-satellite quantum key distribution. *Nat. Phot.*, 7(5):387–393, May 2013.

[76] J.-P. Bourgoin, B. L. Higgins, N. Gigov, C. Holloway, C. J. Pugh, S. Kaiser, M. Cranmer, and T. Jennewein. Free-space quantum key distribution to a moving receiver. *Opt. Express*, 23(26):33437–33447, Dec 2015.

[77] R. J. Hughes, W. T. Buttler, P. G. Kwiat, S. K. Lamoreuax, G. L. Morgan, J. E. Nordholt, and C. G. Peterson. Quantum cryptography for secure satellite communications. In *2000 IEEE Aerospace Conference. Proceedings (Cat. No.00TH8484)*, volume 1, pages 191–200, 2000.

[78] Z. Tang, R. Chandrasekara, Y. Y. Sean, C. Cheng, C. Wildfeuer, and A. Ling. Near-space flight of a correlated photon system. *Sci. Rep.*, 4:6366, 2014.

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

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

[81] P. Villoresi, T. Jennewein, F. Tamburini, M. Aspelmeyer, C. Bonato, R. Ursin, C. Pernechele, V. Luceri, G. Bianco, A. Zeilinger, and C. Barbieri. Experimental verification of the feasibility of a quantum channel between space and Earth. *New J. Phys.*, 10(3):033038, 2008.

[82] R. Etengu, F. M. Abbou, H. Y. Wong, A. Abid, N. Nortiza, and A. Setharaman. Performance comparison of BB84 and B92 satellite-based free space quantum optical communication systems in the presence of channel effects. *J. Opt. Comm.*, 32:37–47, April 2011.

[83] E. Meyer-Scott, Z. Yan, A. MacDonald, J.-P. Bourgoin, H. Hübel, and T. Jennewein. How to implement decoy-state quantum key distribution for a satellite uplink with 50-dB channel loss. *Phys. Rev. A*, 84:062326, Dec 2011.

[84] H. Xin. Chinese academy takes space under its wing. *Science*, 332:904, 2011.

[85] H. Takenaka, M. Toyoshima, Y. Takayama, Y. Koyama, and M. Akioka. Experiment plan for a small optical transponder onboard a 50 kg-class small satellite. In *2011 International Conference on Space Optical Systems and Applications*, pages 113–116, 2011.

[86] J. Yin, Y. Cao, S.-B. Liu, G.-S. Pan, J.-H. Wang, T. Yang, Z.-P. Zhang, F.-M. Yang, Y.-A. Chen, C.-Z. Peng, and J.-W. Pan. Experimental quasi-single-photon transmission from satellite to earth. *Opt. Express*, 21(17):20032–20040, Aug 2013.

[87] G. Vallone, D. Dequal, M. Tomasin, M. Schiavon, F. Vedovato, D. Bacco, S. Gaiarin, G. Bianco, V. Luceri, and P. Villoresi. Satellite quantum communication towards GEO distances. *Proc. SPIE*, 9900:99000J–99000J–8, 2016.

[88] T. Jennewein, J.-P. Bourgoin, B. Higgins, C. Holloway, E. Meyer-Scott, C. Erven, B. Heim, Z. Yan, H. Hbel, G. Weihs, E. Choi, I. D'Souza, D. Hudson, and R. Laflamme. QEYSSAT: a mission proposal for a quantum receiver in space. *Proc. SPIE*, 8997:89970A–89970A–7, 2014.

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

[90] K. Durak, A. Villar, B. Septriani, Z. Tang, R. Chandrasekara, R. Bedington, and A. Ling. The next iteration of the small photon entangling quantum system (SPEQS-2.0). *Proc. SPIE*, 9762:976209–976209–9, 2016.

[91] Z. Tang, R. Chandrasekara, Y. C. Tan, C. Cheng, L. Sha, G. C. Hiang, D. K. L. Oi, and A. Ling. Generation and analysis of correlated pairs of photons aboard a nanosatellite. *Phys. Rev. Applied*, 5:054022, May 2016.

[92] Z. Tang, R. Chandrasekara, Y. C. Tan, C. Cheng, K. Durak, and A. Ling. The photon pair source that survived a rocket explosion. *Scientific Reports*, 6:25603 EP –, May 2016. Article.

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

[94] Quantum optics lifts off. *Nat. Phot.*, 10:689, 2016.

[95] J. Yin, Y. Cao, Y.-H. Li, S.-K. Liao, L. Zhang, J.-G. Ren, W.-Q. Cai, W.-Y. Liu, B. Li, H. Dai, G.-B. Li, Q.-M. Lu, Y.-H. Gong, Y. Xu, S.-L. Li, F.-Z. Li, Y.-Y. Yin, Z.-Q. Jiang, M. Li, J.-J. Jia, G. Ren, D. He, Y.-L. Zhou, X.-X. Zhang, N. Wang, X. Chang, Z.-C. Zhu, N.-L. Liu, Y.-A. Chen, C.-Y. Lu, R. Shu, C.-Z. Peng, J.-Y. Wang, and J.-W. Pan. Satellite-based entanglement distribution over 1200 kilometers. *Science*, 356(6343):1140–1144, 2017.

[96] H.-L. Yong L. Zhang S.-K. Liao J. Yin W.-Y. Liu W.-Q. Cai M. Yang L. Li K.-X. Yang X. Han Y.-Q. Yao J. Li H.-Y. Wu S. Wan L. Liu D.-Q. Liu Y.-W. Kuang Z.-P. He P. Shang C. Guo R.-H. Zheng K. Tian Z.-C. Zhu N.-L. Liu C.-Y. Lu R. Shu Y.-A. Chen C.-Z. Peng J.-Y. Wang J.-W. Pan J.-G. Ren, P. Xu. Ground-to-satellite quantum teleportation. *arXiv:1707.00934*, 2017.

[97] W.-Y. Liu L. Zhang-Y. Li J.-G. Ren-J. Y. Q. Shen Y. Cao Z.-P. Li F.-Z. Li X.-W. Chen-L.-H. Sun J.-J. Jia J.-C. Wu X.-J. Jiang-J.-F. Wang-Y.-M. Huang-Q. Wang Y.-L. Zhou L. Deng-T. Xi L. Ma T. Hu Q. Zhang-Y.-A. Chen-N.-L. Liu X.-B. Wang Z.-C. Zhu C.-Y. Lu R. Shu-C.-Z. Peng J.-Y. Wang J.-W. Pan S.-K. Liao, W.-Q. Cai. Satellite-to-ground quantum key distribution. *arXiv:1707.00542*, 2017.

[98] R. Tyson. *Principles of Adaptive Optics*. CRC Press, 3rd ed. edition, 2010.

[99] R. E. Hufnagel. Variations of Atomspheric Turbulence. In *Digest of Topical Meeting on Optical Propagation Through Turbulence, OSA Technical Digest Series (Optical Society of America, Washinton, D.C.)*, pages WA1–1–WA1–4, 1974.

[100] J. C. Kaimal, J. C. Wyngaard, D. A. Haugen, O. R. Cot, Y. Izumi, S. J. Caughey, and C. J. Readings. Turbulence structure in the convective boundary layer. *Journal of the Atmospheric Sciences*, 33(11):2152–2169, 1976.

[101] D. L. Walters and K. E. Kunkel. Atmospheric modulation transfer function for desert and mountain locations: the atmospheric effects on r0. *J. Opt. Soc. Am.*, 71(4):397–405, Apr 1981.

[102] R. E. Good, R. R. Beland, E. A. Murphy, J. H. Brown, and E. M. Dewan. Atmospheric models of optical turbulence. *Proc. SPIE*, 0928:165–186, 1988.

[103] D. Dayton, J. Gonglewski, B. Pierson, and B. Spielbusch. Atmospheric structure function measurements with a shack–hartmann wave-front sensor. *Opt. Lett.*, 17(24):1737–1739, Dec 1992.

[104] N. Védrenne, V. Michau, C. Robert, and J.-M. Conan. Cn2 profile measurement from shack-hartmann data. *Opt. Lett.*, 32(18):2659–2661, Sep 2007.

[105] D. L. Fried. Statistics of a geometric representation of wavefront distortion. *J. Opt. Soc. Am.*, 55(11):1427–1431, Nov 1965.

[106] J. S. Accetta and D. L. Shumaker. *The Infrared and electro-optical systems handbook*, volume 2. Infrared Information Analysis Center and SPIE Optical Engineering Press, 1993.

[107] E. J. McCartney. *Optics of the atmosphere: Scattering by molecules and particles*. 1976.

[108] Bourgoin, J.-P. *Experimental and theoretical demonstration of the feasibility of global quantum cryptography using satellites*. PhD thesis, 2014.

[109] F. Marsili, V. B. Verma, J. A. Stern, A. E. Harrington, A. E. Lita, T. Gerrits, I. Vayshenker, B. Baek, M. D. Shaw, R. P. Mirin, and S. W. Nam. Detecting single infrared photons with 93% system efficiency. *Nat. Phot.*, 7(3):210–214, Mar 2013.

[110] Canadian Space Agency. Usefulness of Adaptive Optics for QKD. grant 2011-2012.

[111] R. W. Duffner. Revolutionary imaging: Air force contributions to laser guide star adaptive optics. *ITEA Journal of Test and Evaluation*, 29(4):341–346, 2008.

[112] A. Roorda. Adaptive optics for studying visual function: A comprehensive review. *Journal of Vision*, 11(5), 2011.

[113] J. W. Armstrong, C. Yeh, and K. E. Wilson. Earth-to-deep-space optical communications system with adaptive tilt and scintillation correction by use of near-Earth relay mirrors. *Opt. Lett.*, 23, 1998.

[114] von F. Zernike. Beugungstheorie des schneidenver-fahrens und seiner verbesserten form, der phasenkontrastmethode. *Physica*, 1(712):689 – 704, 1934.

[115] J. W. Hardy. *Adaptive Optics for Astronomical Telescopes*. Oxford series in optical and imaging sciences. Oxford University Press, 1998.

[116] S. Chueca, B. Garca-Lorenzo, C. Muoz-Tun, and J. J. Fuensalida. Statistics and analysis of high-altitude wind above the canary islands observatories. *Monthly Notices of the Royal Astronomical Society*, 349(2):627–631, 2004.

[117] D.H. Tofsted, S.G. O'Brien, G.T. Vaucher, ARMY RESEARCH LAB WHITE SANDS MISSILE RANGE NM COMPUTATIONAL, and INFORMATION SCIENCE DIRECTORATE. *An Atmospheric Turbulence Profile Model for Use in Army Wargaming Applications I.* Defense Technical Information Center, 2006.

[118] J. L. Bufton. Comparison of vertical profile turbulence structure with stellar observations. *Appl. Opt.*, 12(8):1785–1793, Aug 1973.

[119] Cottrell P. L. C. Mohr J. L. M., Johnston R. A. J. Optical turbulence measurements and models for mount john university observatory. *Publications of the Astronomical Society of Australia*, 27:347–359, 2010.

[120] R. L. Fante. Electromagnetic beam propagation in turbulent media. *Proceedings of the IEEE*, 63(12):1669–1692, Dec 1975.

[121] F. Dios, J. Antonio Rubio, A. Rodríguez, and A. Comerón. Scintillation and beam-wander analysis in an optical ground station-satellite uplink. *Appl. Opt.*, 43(19):3866–3873, Jul 2004.

[122] M. Jeganathan, K. Wilson, and Lesh J. R. Preliminary Analysis of Fluctuations in the Received Uplink-Beacon-Power Data Obtained from GOLD Experiments. In *The Telecommunications and Data Acquisition Progress Report*, pages 20–32, JPL, Pasadena, California, 1996.

[123] H. T. Yura. Short-term average optical-beam spread in a turbulent medium. *J. Opt. Soc. Am.*, 63(5):567–572, May 1973.

[124] G. A. Tyler. Bandwidth considerations for tracking through turbulence. *J. Opt. Soc. Am. A*, 11(1):358–367, Jan 1994.

[125] S. S. Olivier, C. E. Max, D. T. Gavel, and J. M. Brase. Tip-tilt compensation: Resolution limits for ground-based telescopes using laser guide star adaptive optics. *Astrophysical Journal*, 407(1):428–439, 1993.

[126] P. Wizinowich. Keck adaptive optics note 051 keck adaptive optics error budget. https://www2.keck.hawaii.edu/optics/aowg/docs/kaon051.pdf, 1995.

[127] R. Teoste, J. A. Daley, Jr., R. N. Capes, Jr., J. J. Alves, and M. D. Zimmerman. *Measurements of tilt anisoplanatism at the Firepond Facility*. November 1988.

[128] V. N. Mahajan. Strehl ratio for primary aberrations in terms of their aberration variance. *J. Opt. Soc. Am.*, 73(6):860–861, Jun 1983.

[129] D. P. Greenwood. Bandwidth specification for adaptive optics systems. *J. Opt. Soc. Am.*, 67(3):390–393, Mar 1977.

[130] A. Glindemann, S. Hippler, T. Berkefeld, and W. Hackenberg. Adaptive optics on large telescopes. *Experimental Astronomy*, 10(1):5–47, 2000.

[131] R. J. Noll. Zernike polynomials and atmospheric turbulence. *J. Opt. Soc. Am.*, 66(3):207–211, Mar 1976.

[132] G. A. Tyler. Turbulence-induced adaptive-optics performance degradation: evaluation in the time domain. *J. Opt. Soc. Am. A*, 1(3):251–262, Mar 1984.

[133] S. Kaiser. *Quantum key distribution devices: How to make them and how to break them*. PhD thesis, University of Waterloo, Department of Physics and Astronomy, 2017.

[134] Canadian Space Agency. Quantum Key Distribution Receiver. contract no. 9F063-120711/002/MTB.

[135] K. Aoki, Y. Yanagita, H. Kuroda, and K. Shiratama. Wide-range fine pointing mechanism for free-space laser communications. *Proc. SPIE*, 5160:495–506, 2004.

[136] M. Meftah, A. Irbah, R. Le Letty, A. Bataille, E. Ducourt, G. Poiet, and M. Privat. The PICARD/SODISM Pointing Mechanism: From the Design to the Flight Performances. In *ESMATS 2011, 14th European Space Mechanisms and Tribology Symposium 2011*, page 8 pp., Constance, Germany, September 2011. ESA.

[137] P. Bandera. A fine pointing mechanism for intersatellite laser communication. In *Space Mechanisms and Tribology, Proceedings of the 8th European Symposium*, volume 438, pages 61–65, 1999.

[138] S. Shimizu, K. Fukushima, K. Kodeki, T. Ando, and T. Araki. Development of fine pointing mechanism for optical inter-satellite communication. In *Proc. International Conference on Space Optical Systems and Applications*, pages P–5, 2014.

[139] S. Lee, J. W. Alexander, and M. Jeganathan. Pointing and tracking subsystem design for optical communications link between the international space station and ground. *Proc. SPIE*, 3932:150–157, 2000.

[140] G. G. Ortiz, A. Portillo, S. Lee, and J. M. Ceniceros. Functional demonstration of accelerometer-assisted beacon tracking. *Proc. SPIE*, 4272:112–117, 2001.

[141] S. Lee, J. W. Alexander, and G. G. Ortiz. Submicroradian pointing system design for deep-space optical communications. *Proc. SPIE*, 4272:104–111, 2001.

[142] T. Aruga, K. Araki, T. Igarashi, F. Imai, Y. Yamamoto, and H. Sakagami. Earth-to-space laser beam transmission for spacecraft attitude measurement. *Appl. Opt.*, 23(1):143–147, Jan 1984.

[143] A. Skullestad. Pointing mechanism for optical communication. In *Space Mechanisms and Tribology, Proceedings of the 8th European Symposium*, volume 438, pages 57–60, 1999.

[144] C. Fuchs. Fine tracking system for aeronautical fso links. In *15th Ka and Broadband Communications, Navigation and Earth Observation Conference*, September 2009.

[145] F. Moll, S. Nauerth, C. Fuchs, J. Horwath, M. Rau, and H. Weinfurter. Communication system technology for demonstration of BB84 quantum key distribution in optical aircraft downlinks. *Proc. SPIE*, 8517:851703–851703–8, 2012.

[146] F. M. Pranajaya and R. E. Zee. The NEMO bus: a third generation high-performance nanosatellite for earth monitoring and observation. In *24th Annual AIAA/USU Conference on Small Satellites*, pages SSC10–VI–8, 2010.

[147] Canadian Space Agency. APT quantum enrcyption satellite. Solicitation no. 9F043-110522/A.

[148] C. M. Pong, S. Lim, M. W. Smith, D. W. Miller, J. S. Villaseor, and S. Seager. Achieving high-precision pointing on exoplanetsat: initial feasibility analysis. *Proc. SPIE*, 7731:77311V–77311V–16, 2010.

[149] M. Toyoshima, H. Takenaka, Y. Shoji, Y. Takayama, Y. Koyama, and H. Kunimori. Polarization measurements through space-to-ground atmospheric propagation paths by using a highly polarized laser source in space. *Opt. Express*, 17(25):22333–22340, Dec 2009.

[150] M. Toyoshima and K. Araki. Effects of time averaging on optical scintillation in a ground-to-satellite atmospheric propagation. *Appl. Opt.*, 39(12):1911–1919, Apr 2000.

[151] M. Toyoshima, Y. Takayama, T. Takahashi, K. Suzuki, S. Kimura, K. Takizawa, T. Kuri, W. Klaus, M. Toyoda, H. Kunimori, T. Jono, and K. Arai. Ground-to-satellite laser communication experiments. *IEEE Aerospace and Electronic Systems Magazine*, 23(8):10–18, Aug 2008.

[152] J. R. Wertz and W. J. Larson. *Space Mission Analysis and Design*. Space Technology Library. Springer Netherlands, 1999.

[153] J. Strohbehn and S. Clifford. Polarization and angle-of-arrival fluctuations for a plane wave propagated through a turbulent medium. *IEEE Transactions on Antennas and Propagation*, 15(3):416–421, May 1967.

[154] D. H. Höhn. Depolarization of a laser beam at 6328 å due to atmospheric transmission. *Appl. Opt.*, 8(2):367–369, Feb 1969.

[155] E. Collett and R. Alferness. Depolarization of a laser beam in a turbulent medium. *J. Opt. Soc. Am.*, 62(4):529–533, Apr 1972.

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

[157] Z. Yan, E. Meyer-Scott, J.-P. Bourgoin, B. L. Higgins, N. Gigov, A. MacDonald, H. Hübel, and T. Jennewein. Novel high-speed polarization source for decoy-state BB84 quantum key distribution over free space and satellite links. *J. Lightwave Technol.*, 31(9):1399–1408, May 2013.

[158] R. W. Boyd. *Nonlinear Optics, Third Edition*. Academic Press, 3rd edition, 2008.

[159] N. Jain, E. Anisimova, I. Khan, V. Makarov, C. Marquardt, and G. Leuchs. Trojan-horse attacks threaten the security of practical quantum cryptography. *New J. Phys.*, 16(12):123030, 2014.

[160] S. Sajeed, P. Chaiwongkhot, J.-P. Bourgoin, T. Jennewein, N. Lütkenhaus, and V. Makarov. Security loophole in free-space quantum key distribution due to spatial-mode detector-efficiency mismatch. *Phys. Rev. A*, 91:062301, Jun 2015.

[161] GHGSat Inc. GHGSat. http://www.ghgsat.com/.

[162] National Research Council of Canada. Towards Quantum Sensing with Optical Photons. contract no. 879726.

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

[164] J.-P. Bourgoin, N. Gigov, B. L. Higgins, Z. Yan, E. Meyer-Scott, A. K. Khandani, N. Lütkenhaus, and T. Jennewein. Experimental quantum key distribution with simulated ground-to-satellite photon losses and processing limitations. *Phys. Rev. A*, 92:052339, Nov 2015.

[165] S. Lloyd. Enhanced sensitivity of photodetection via quantum illumination. *Science*, 321(5895):1463–1465, 2008.

[166] J. H. Shapiro. Defeating passive eavesdropping with quantum illumination. *Phys. Rev. A*, 80:022320, Aug 2009.

[167] Z. Zhang, M. Tengner, T. Zhong, F. N. C. Wong, and J. H. Shapiro. Entanglement's benefit survives an entanglement-breaking channel. *Phys. Rev. Lett.*, 111:010501, Jul 2013.

[168] S. Barzanjeh, S. Guha, C. Weedbrook, D. Vitali, J. H. Shapiro, and S. Pirandola. Microwave quantum illumination. *Phys. Rev. Lett.*, 114:080503, Feb 2015.

[169] E. Anisimova, B. L. Higgins, J.-P. Bourgoin, M. Cranmer, E. Choi, D. Hudson, L. P. Piche, A. Scott, V. Makarov, and T. Jennewein. Mitigating radiation damage of single photon detectors for space applications. *arXiv:1702.01186*, 2017.

[170] J. G. Lim, E. Anisimova, B. L. Higgins, J.-P. Bourgoin, T. Jennewein, and V. Makarov. Laser annealing heals radiation damage in avalanche photodiodes. *EPJ Quantum Technology*, 4(1):11, 2017.

[171] C. H. Bennet, G. Brassard, and N. D. Mermin. Quantum cryptography without Bell's theorem. *Phys. Rev. Lett.*, 68:557–559, 1992.

[172] T. Jennewein, C. Grant, E. Choi, C. Pugh, C. Holloway, J.-P. Bourgoin, H. Hakima, B. Higgins, and R. Zee. The NanoQEY mission: ground to space quantum key and entanglement distribution using a nanosatellite. *Proc. SPIE*, 9254:925402–925402–6, 2014.

[173] FedDev. Feasibility of NanoQEY mission. project no. 802020.

[174] University of Toronto Institute for Aerospace Studies Space Flight Laboratory. NEMO bus. https://www.utias-sfl.net/?page_id=89, 2014.

[175] T. D. Henson and G. K. Torrington. Space radiation testing of radiation-resistant glasses and crystals. *Proc. SPIE*, 4452:54–65, 2001.

[176] BMV Optical Technologies. http://www.bmvoptical.com/, 2017.

[177] D. M. Winker, M. A. Vaughan, A. Omar, Y. Hu, K. A. Powell, Z. Liu, W. H. Hunt, and S. A. Young. Overview of the calipso mission and caliop data processing algorithms. *Journal of Atmospheric and Oceanic Technology*, 26(11):2310–2323, 2009.

[178] G. Osteria, D. Campana, G. Barbarino, M. Boscherini, W. Menn, J. Mitchell, G. Rossi, S. Russo, M. Simon, and R. Streitmatter. The time-of-flight system of the {PAMELA} experiment on satellite. *Nuclear Instruments and Methods in Physics Research Section A: Accelerators, Spectrometers, Detectors and Associated*

Equipment, 535(12):152 – 157, 2004. Proceedings of the 10th International Vienna Conference on Instrumentation.

[179] Y. C. Tan, R. Chandrasekara, C. Cheng, and A. Ling. Silicon avalanche photodiode operation and lifetime analysis for small satellites. *arXiv:1306.6773*, 2013.

[180] *Photomultiplier Tubes*. Hamamatsu Photonics K. K., 3rd edition, 2007.

[181] Hamamatsu H7422 series datasheet. http://www.hamamatsu.com/eu/en/product/alpha/P/3003/3044/H7422-40/index.html.

[182] A. Berk, G. P. Anderson, P. K. Acharya, L. S. Bernstein, L. Muratov, J. Lee, M. J. Fox, S. M. Adler-Golden, J. H. Chetwynd, M. L. Hoke, R. B. Lockwood, T. W. Cooley, and J. A. Gardner. Modtran5: a reformulated atmospheric band model with auxiliary species and practical multiple scattering options. *Proc. SPIE*, 5655:88–95, 2005.

[183] S. Y. Kotchenova, E. F. Vermote, R. Levy, and A. Lyapustin. Radiative transfer codes for atmospheric correction and aerosol retrieval: intercomparison study. *Appl. Opt.*, 47(13):2215–2226, May 2008.

[184] C. Grant. Technical note on radiator thermal modelling.

[185] Zedboard. http://www.zedboard.org/product/zedboard.

Appendix A

Code for Adaptive Optics Effect on QKD

```
#Code studying the effect Adaptive Optics on QKD links
#Definition section written by Brendon Higgins, calculation section ...
    written by Christopher Pugh
#2014-2017

from math import *
import numpy as np
from scipy import integrate, constants, optimize
import matplotlib.pyplot as plt

#Sum of squares
def rtsumsq(xs):
    return sqrt(sum([x**2 for x in xs]))

#Earth parameters
earth_radius = 6371e3 # m (mean)
earth_mass = 5.97219e24 # kg

sec = lambda x: 1./cos(x)

#Calculates the angular velocity of the satellite
def sat_angular_vel(planet_mass, orbit_radius):
    return sqrt(constants.G*planet_mass/orbit_radius**3)

#Calculate the angular location of the satellite at the planet's ...
    center given
#its angle from zenith, assuming that zenith is aligned to the origin.
```

```
26 def sat_angular_loc_from_zenith(zenith_angle, orbit_height, ...
       planet_radius):
27     return zenith_angle - ...
           asin(planet_radius*sin(zenith_angle)/(planet_radius + ...
           orbit_height))
28
29 #Calculates the satellite's previous angle based on the flight time ...
       of photons between previous and current locations
30 def sat_zenith_from_angular_loc(angular_loc, orbit_height, ...
       planet_radius):
31     return atan2(sin(angular_loc), cos(angular_loc) - ...
           planet_radius/(planet_radius + orbit_height))
32
33 #Calculates the distance from the ground station to the satellite
34 def sat_dist_from_zenith(zenith_angle, orbit_height, planet_radius):
35     a = 2.
36     b = 4*planet_radius*cos(zenith_angle)
37     c = -2*orbit_height*(orbit_height + 2*planet_radius)
38     return (-b + sqrt(b**2 - 4*a*c))/2./a
39
40 #Calculates the satellite's previous distance
41 def sat_dist_from_angular_loc(angular_loc, orbit_height, planet_radius):
42     l = planet_radius + orbit_height
43     return sqrt(l**2 + planet_radius**2 - ...
           2*planet_radius*l*cos(angular_loc))
44
45 #Calculate the angular sweep between the (present) zenith angle and ...
       the (prior)
46 #zenith angle the satellite must have been at such that light could ...
       propagate
47 #from the prior position, to ground, then to the present position in ...
       the time
48 #the satellite orbited between those two positions.
49 def sat_angular_sweep(zenith_angle, orbit_height, planet_radius, ...
       planet_mass):
50     omega = sat_angular_vel(planet_mass, orbit_height + planet_radius)
51     present_loc = sat_angular_loc_from_zenith(zenith_angle, ...
           orbit_height, planet_radius)
52     present_dist = sat_dist_from_zenith(zenith_angle, orbit_height, ...
           planet_radius)
53     prior_loc = lambda t: present_loc + omega*t
54     prior_zenith = lambda t: ...
           sat_zenith_from_angular_loc(prior_loc(t), orbit_height, ...
           planet_radius)
```

```
    prior_dist = lambda t: sat_dist_from_angular_loc(prior_loc(t), ...
        orbit_height, planet_radius)
    e = lambda t: (present_dist + prior_dist(t))/constants.c - t
    t = optimize.brentq(e, 0., 2*(orbit_height + ...
        2*planet_radius)/constants.c)
    return prior_zenith(t) - zenith_angle

#Hufnagel-Valley model parameters
hv_5_7_model = {'a': 17e-15, 'h_a': 100, 'b': 27e-17, 'h_b': 1500, ...
    'c': 3.59e-53, 'h_c': 1000}
hv_10_10_model = {'a': 4.5e-15, 'h_a': 100, 'b': 9e-17, 'h_b': 1500, ...
    'c': 2.0e-53, 'h_c': 1000}
hv_15_12_model = {'a': 2.0e-15, 'h_a': 100, 'b': 7e-17, 'h_b': 1500, ...
    'c': 1.54e-53, 'h_c': 1000}
tenerife_model = {'a': 9.42e-15, 'h_a': 100, 'b': 27e-17, 'h_b': ...
    1500, 'c': 2.50e-53, 'h_c': 1000}
vacuum_model = {'a': 0, 'h_a': 1, 'b': 0, 'h_b': 1, 'c': 0, 'h_c': 1}

#Atmospheric structure function
def csq(h, a, h_a, b, h_b, c, h_c, d = 0, h_d = 0, t = 1):
    r = 0.
    if a != 0:
        r += a*exp(-h/float(h_a))
    if b != 0:
        r += b*exp(-h/float(h_b))
    if c != 0:
        r += c*h**10*exp(-h/float(h_c))
    if d != 0:
        r += d*exp(-(h - h_d)**2/(2.*t**2))
    return r

#Fried's coherence length
def r_0(zenith_angle, orbit_height, k, atm_model):
    r = 0.423*k**2*integrate.quad(lambda h: csq(h, ...
        **atm_model)*(1-h/float(orbit_height))**(5./3.), 0, ...
        orbit_height, epsabs=1e-18, limit=1000)[0]/cos(zenith_angle)
    return r**(-3./5.) if r != 0 else float('inf')

#Diffraction beam width squared
def beamwidth_diff_sq(w_0, z_0, z):
    return w_0**2*(1. + (z/float(z_0))**2)

#Diffraction beam width
def beamwidth_diff(w_0, z_0, z):
```

```
91      return sqrt(beamwidth_diff_sq(w_0, z_0, z))
92
93  #Long term turbulence limited beam width
94  def beamwidth_lt(w_0, z_0, r_0, z, k):
95      return sqrt(beamwidth_diff_sq(w_0, z_0, z) + 2*(4.*z/k/r_0)**2)
96
97  #Long term turbulence beam width with diffraction beam width removed
98  def beamwidth_nodiff_lt(z, k, r_0):
99      return sqrt(2*(4.*z/k/r_0)**2)
100
101 #Short term turbulence limtied beam width
102 def beamwidth_st(w_0, z_0, r_0, z, k):
103     return sqrt(beamwidth_diff_sq(w_0, z_0, z) + 2*(4.2*z*(1 - ...
            0.26*(r_0/w_0)**(1./3.))/k/r_0)**2)
104
105 #Link efficiency for tip/tilt AO
106 def link_efficiency(trans_efficiency, rec_efficiency, rec_diameter, ...
        zenith_transmittance, zenith_angle, w, corr_factor):
107     return 10*log10(trans_efficiency*rec_efficiency
108         *zenith_transmittance**sec(zenith_angle)
109             *(rec_diameter/w)**2*corr_factor)
110
111 #Tracking frequency for centroid anisoplanatism error
112 def tracking_freq(wavelength, trans_diameter, zenith_angle, ...
        orbit_height, atm_model, wind_speed_fn, wind_speed):
113     i = integrate.quad(lambda h: csq(h, ...
            **atm_model)*wind_speed_fn(h,wind_speed)**2, 0, orbit_height, ...
            epsabs=1e-18, limit=1000)[0]/cos(zenith_angle)
114     return 0.331*sqrt(i)/trans_diameter**(1./6.)/wavelength
115
116 #Greenwood frequency for higher order phase AO delay error
117 def greenwood_freq(wavelength, zenith_angle, orbit_height, atm_model, ...
        wind_speed_fn, wind_speed):
118     return 2.31*wavelength**(-6./5.)*(integrate.quad(lambda h: csq(h, ...
            **atm_model)*wind_speed_fn(h,wind_speed)**(5./3.), 0, ...
            orbit_height, epsabs=1e-18, ...
            limit=1000)[0]/cos(zenith_angle))**(3./5.)
119
120 #Bufton wind model
121 def bufton_wind(h, wind_speed, vg = 5., hpk = 9.4e3, hscale = 4.8e3):
122     return vg + wind_speed*exp(-((h - hpk)/hscale)**2)
123
124 #Circular aperture function for tilt anisoplanatism error
125 def circular_aperture_w(h, trans_diameter, Δ_tilt, zenith_angle):
```

```
126     fivesix = 5./6.
127     fivethree = 5./3.
128     s = h*Δ_tilt/trans_diameter/cos(zenith_angle)
129     ssq = s*s
130     sft = s**fivethree
131     def q(u, w):
132         return ((0.5*(u**2 + 2*u*s*cos(w) + ssq)**fivesix
133             + 0.5*(u**2 - 2*u*s*cos(w) + ssq)**fivesix - u**fivethree ...
                    - sft)
134             *u*(acos(u) - (3*u - 2*u**3)*sqrt(1 - u**2)))
135     return integrate.dblquad(lambda u, w: q(u, w), 0., 2*pi, lambda ...
            _: 0., lambda _: 1., epsabs=1e-18)[0]
136
137 #Signal to noise error of the position sensitive detector
138 sigma_snr = 0.15e-6
139
140 #Tilt time delay error
141 def sigma_wander_delay(wavelength, trans_diameter, loop_bandwidth, ...
        zenith_angle, orbit_height, atm_model, wind_speed_fn, wind_speed):
142     return tracking_freq(wavelength, trans_diameter, zenith_angle, ...
            orbit_height, atm_model, wind_speed_fn, ...
            wind_speed)*wavelength/loop_bandwidth/trans_diameter
143
144 #Centroid anisoplanatism error
145 def sigma_alias(wavelength, trans_diameter, r_0):
146     return ...
            5.51e-2*wavelength/trans_diameter*(trans_diameter/r_0)**(5./6.)
147
148 #Tilt anisoplanatism error
149 def sigma_ani_tilt(trans_diameter, Δ_tilt, zenith_angle, ...
        orbit_height, atm_model):
150     return 6.14*sqrt(integrate.quad(lambda h: csq(h, ...
            **atm_model)*circular_aperture_w(h, trans_diameter, Δ_tilt, ...
            zenith_angle), 0, orbit_height, epsabs=1e-18, ...
            limit=1000)[0]/cos(zenith_angle))/trans_diameter**(1./6.)
151
152 #Isoplanatic angle
153 def theta_0(k, zenith_angle, orbit_height, atm_model):
154     return ...
            (2.91*k**2*cos(zenith_angle)**(-8./3.)*integrate.quad(lambda ...
            h: csq(h, **atm_model)*h**(5./3.), 0, orbit_height, ...
            epsabs=1e-18, limit=1000)[0])**(-3./5.)
155
156 #Phase anisoplanatism error
```

```
157 def sigma_ani_phase(k, zenith_angle, orbit_height, planet_radius, ...
        planet_mass, atm_model):
158     theta = sat_angular_sweep(zenith_angle, orbit_height, ...
            planet_radius, planet_mass)
159     #print theta
160     theta0 = theta_0(k, zenith_angle, orbit_height, atm_model)
161     #print theta0
162     return (theta/theta0)**(5./6.)
163
164 #Phase time delay error
165 def sigma_ao_delay(wavelength, loop_bandwidth, zenith_angle, ...
        orbit_height, atm_model, wind_speed_fn, wind_speed):
166     return (greenwood_freq(wavelength, zenith_angle, orbit_height, ...
            atm_model, wind_speed_fn, wind_speed)/loop_bandwidth)**(5./6.)
167
168 #Spatial fitting error
169 def sigma_fit(trans_diameter, r_0, zernike_modes):
170     return sqrt(0.2944*zernike_modes**(-sqrt(3.)/2.)
171         *(trans_diameter/r_0)**(5./3.))
172
173 #Laser guide star cone error
174 def sigma_cone(trans_diameter, wavelength, orbit_height, ...
        zenith_angle, LGS_height, atm_model):
175     d0 = (wavelength**(6./5.)
176             *cos(zenith_angle)**(3./5.)*(19.77*integrate.quad(lambda ...
                h: csq(h, **atm_model)*(h/LGS_height)**(5./3.), 0, ...
                orbit_height, epsabs=1e-18, limit=1000)[0])**(-3./5.))
177     return (trans_diameter/d0)**(5./6.)
178
179 #I, correction factor for residual jitter
180 def jitter_energy_loss_factor(w, z, sigmas):
181     div_angle = w/z
182     beta = div_angle**2/sum([x**2 for x in sigmas])/8.
183     return beta/(beta + 1)
184
185 #Strehl ratio
186 def strehl_approx(sigmas):
187     #print exp(-sum([x**2 for x in sigmas]))
188     return exp(-sum([x**2 for x in sigmas]))
189
190 #Link efficiency for full AO correction
191 def link_efficiency_ao(trans_efficiency, rec_efficiency, ...
        rec_diameter, zenith_transmittance, zenith_angle, w_diff, i_diff, ...
        w_st, i_st, sigmas):
```

```
192     s = strehl_approx(sigmas)
193     return 10*log10(trans_efficiency*rec_efficiency
194         *zenith_transmittance**sec(zenith_angle)*(rec_diameter)**2
195             *(i_diff*s/w_diff**2 + i_st*(1 - s)/w_st**2))
196 
197 #Parameters for AO simulations (in some cases they are overwritten in ...
       the sections)
198 trans_efficiency = 0.5
199 trans_diameter = 0.5
200 rec_efficiency = 0.5
201 rec_diameter = 0.4
202 zenith_transmittance = 0.8
203 orbit_height = 600e3
204 wavelength = 785e-9
205 wind_speed=20
206 #Wave number
207 k = 2*pi/wavelength
208 #Beam waist
209 w_0 = 1./sqrt(2*log(2))*trans_diameter/2.
210 #Rayleigh range
211 z_0 = pi*w_0**2/wavelength
212 
213 loop_bandwidth = 60.
214 zernike_modes = 45.
215 
216 #This section allows one to chose which particular parameters to be ...
       plotted, can choose 1-6
217 if __name__ == "__main__":
218     figures = [4]
219 
220     #Section 1 can be used to plot the long term beam width, ...
           divergence, and link efficiency
221     if 1 in figures:
222 
223         #Defining divergence arrays
224         tot_div=range(0,81)
225         diff_div=range(0,81)
226         turb_div=range(0,81)
227         #Define transmitter diameter and associated beam waist
228         trans_diameter = 0.25
229         w_0 = 1./sqrt(2*log(2))*trans_diameter/2.
230         z_0 = pi*w_0**2/wavelength
231 
232         #Angle from zenith
```

```
233         iss = range(0, 81)
234         #Elevation angle
235         elev=range(90,9,-1)
236         #Fried parameter for various angles from zenith
237         r0s = [r_0(i*pi/180, orbit_height, k, hv_5_7_model) for i in iss]
238         #Distance from ground station to satellite for different ...
                angles from zenith
239         dists = [sat_dist_from_zenith(i*pi/180, orbit_height, ...
                earth_radius) for i in iss]
240
241         #Calculate beam width for different angles from zenith
242         w_d = [beamwidth_diff(w_0, z_0, dists[i]) for i in ...
                range(len(iss))]
243         w_lt=[beamwidth_lt(w_0, z_0, r0s[i], dists[i], k) for i in iss]
244         w_s = [beamwidth_st(w_0, z_0, r0s[i], dists[i], k) for i in ...
                range(len(iss))]
245         w_nodiff=[beamwidth_nodiff_lt(dists[i], k, r0s[i]) for i in ...
                range(len(iss))]
246
247         #Calculate beam divergence for different angles from zenith
248         for i in range(len(iss)):
249             tot_div[i]=w_lt[i]/dists[i]
250             diff_div[i]=w_d[i]/dists[i]
251             turb_div[i]=w_nodiff[i]/dists[i]
252
253         #Calculate total link efficiency for different angles from zenith
254         total = [link_efficiency(trans_efficiency, rec_efficiency, ...
                rec_diameter, zenith_transmittance, i/180.*pi, w_lt[i], ...
                1.) for i in iss]
255         #Calculate atmosphere limited link efficiency for different ...
                angles from zenith
256         atm =   [link_efficiency(trans_efficiency, rec_efficiency, ...
                rec_diameter, zenith_transmittance, i/180.*pi, ...
                w_nodiff[i], 1.) for i in iss]
257         #Calculate diffraction limited link efficiency for different ...
                angles from zenith
258         diff = [link_efficiency(trans_efficiency, rec_efficiency, ...
                rec_diameter, zenith_transmittance, i/180.*pi, w_d[i], 1.) ...
                for i in iss]
259
260         #Plot beam width as a function of elevation angle
261         plt.plot(elev,w_d,label="Diffraction Limited",lw=3.0,c='black')
262         plt.plot(elev,w_nodiff,label="Turbulence Limited",lw=3.0,ls='--')
263         plt.plot(elev,w_lt,label="Total",lw=3.0,ls=':')
```

```
264         plt.xlabel('Elevation [$^\circ$]')
265         plt.ylabel('Beam Width [m]')
266         plt.legend(loc=1)
267 
268         #Plot beam divergence as a function of elevation angle
269         #plt.plot(elev,diff_div,label="Diffraction ...
                Limited",lw=3.0,c='black')
270         #plt.plot(elev,turb_div, label="Turbulence ...
                Limited",lw=3.0,ls='--')
271         #plt.plot(elev,tot_div, label="Total",lw=3.0,ls=':')
272         #plt.ticklabel_format(style='sci',axis='y',scilimits=(0,0))
273         #plt.xlabel('Elevation [$^\circ$]')
274         #plt.ylabel('Beam divergence [rad]')
275         #plt.legend(loc=1)
276 
277         #Plot link efficiency as a function of elevation angle
278         #plt.plot(elev,diff,label="Diffraction Limited",lw=3.0,c='black')
279         #plt.plot(elev,atm, label="Turbulence Limited",lw=3.0,ls='--')
280         #plt.plot(elev,total, label="Total",lw=3.0,ls=':')
281         #plt.xlabel('Elevation [$^\circ$]')
282         #plt.ylabel('Link efficiency [dB]')
283         #plt.legend(loc=4)
284 
285 
286         plt.show()
287 
288     #Section 2 can be used to calculate and plot the tip/tilt errors ...
            as well as the link efficiency due to these
289     #All calculations are done for zenith in this section
290     if 2 in figures:
291 
292         #Select the system bandwidth
293         band=20.
294         #dia=[0.08,0.25,0.42,0.6,0.85]
295         #Transmitter diameters
296         dia=np.arange(0.05,1,0.01)
297 
298         #Tip/tilt delay error
299         sdelay=[sigma_wander_delay(wavelength, i, band, 0, ...
                orbit_height, hv_5_7_model, bufton_wind, wind_speed)for i ...
                in dia]
300         #Tip/tilt anisoplanatism error
301         sant = [sigma_ani_tilt(i, 50e-6, 0, orbit_height, ...
                hv_5_7_model) for i in dia]
```

```
302         #Centroid anisoplanatism error
303         sal = [sigma_alias(wavelength, i, r_0(0, orbit_height, k, ...
                hv_5_7_model)) for i in dia]
304         #Signal to noise sensor error
305         ss = [sigma_snr for i in dia]
306         #Total combined error
307         stot = [rtsumsq([sdelay[i], sal[i], sant[i], ss[i]]) for i in ...
                range(len(dia))]
308
309         #Calculate the tip/tilt delay error for various bandwidths
310         sdelay1=[sigma_wander_delay(wavelength, i, 20, 0, ...
                orbit_height, hv_5_7_model, bufton_wind, wind_speed)for i ...
                in dia]
311         sdelay2=[sigma_wander_delay(wavelength, i, 40, 0, ...
                orbit_height, hv_5_7_model, bufton_wind, wind_speed)for i ...
                in dia]
312         sdelay3=[sigma_wander_delay(wavelength, i, 60, 0, ...
                orbit_height, hv_5_7_model, bufton_wind, wind_speed)for i ...
                in dia]
313         sdelay4=[sigma_wander_delay(wavelength, i, 80, 0, ...
                orbit_height, hv_5_7_model, bufton_wind, wind_speed)for i ...
                in dia]
314         sdelay5=[sigma_wander_delay(wavelength, i, 100, 0, ...
                orbit_height, hv_5_7_model, bufton_wind, wind_speed)for i ...
                in dia]
315         #Calculate the total errors with different bandwidths
316         stot1 = [rtsumsq([sdelay1[i], sal[i], sant[i], ss[i]]) for i ...
                in range(len(dia))]
317         stot2 = [rtsumsq([sdelay2[i], sal[i], sant[i], ss[i]]) for i ...
                in range(len(dia))]
318         stot3 = [rtsumsq([sdelay3[i], sal[i], sant[i], ss[i]]) for i ...
                in range(len(dia))]
319         stot4 = [rtsumsq([sdelay4[i], sal[i], sant[i], ss[i]]) for i ...
                in range(len(dia))]
320         stot5 = [rtsumsq([sdelay5[i], sal[i], sant[i], ss[i]]) for i ...
                in range(len(dia))]
321         #Adjust the beam size based on the transmitter diameter
322         w_0 = [(1./sqrt(2*log(2))*i/2.)for i in dia]
323         z_0 = [(pi*i**2/wavelength)for i in w_0]
324
325         #Link efficiencies for different bandwidths
326         linke1=[link_efficiency(trans_efficiency, rec_efficiency, ...
                rec_diameter, zenith_transmittance, 0,beamwidth_st(w_0[i], ...
                z_0[i], r_0(0, orbit_height, k, hv_5_7_model), 600000., ...
```

```
            k),jitter_energy_loss_factor(beamwidth_st(w_0[i], z_0[i], ...
            r_0(0, orbit_height, k, hv_5_7_model), 600000., k), ...
            600000, [sdelay1[i],sant[i],sal[i],ss[i]]))for i in ...
            range(len(dia))]
327         linke2=[link_efficiency(trans_efficiency, rec_efficiency, ...
            rec_diameter, zenith_transmittance, 0,beamwidth_st(w_0[i], ...
            z_0[i], r_0(0, orbit_height, k, hv_5_7_model), 600000., ...
            k),jitter_energy_loss_factor(beamwidth_st(w_0[i], z_0[i], ...
            r_0(0, orbit_height, k, hv_5_7_model), 600000., k), ...
            600000, [sdelay2[i],sant[i],sal[i],ss[i]]))for i in ...
            range(len(dia))]
328         linke3=[link_efficiency(trans_efficiency, rec_efficiency, ...
            rec_diameter, zenith_transmittance, 0,beamwidth_st(w_0[i], ...
            z_0[i], r_0(0, orbit_height, k, hv_5_7_model), 600000., ...
            k),jitter_energy_loss_factor(beamwidth_st(w_0[i], z_0[i], ...
            r_0(0, orbit_height, k, hv_5_7_model), 600000., k), ...
            600000, [sdelay3[i],sant[i],sal[i],ss[i]]))for i in ...
            range(len(dia))]
329         linke4=[link_efficiency(trans_efficiency, rec_efficiency, ...
            rec_diameter, zenith_transmittance, 0,beamwidth_st(w_0[i], ...
            z_0[i], r_0(0, orbit_height, k, hv_5_7_model), 600000., ...
            k),jitter_energy_loss_factor(beamwidth_st(w_0[i], z_0[i], ...
            r_0(0, orbit_height, k, hv_5_7_model), 600000., k), ...
            600000, [sdelay4[i],sant[i],sal[i],ss[i]]))for i in ...
            range(len(dia))]
330         linke5=[link_efficiency(trans_efficiency, rec_efficiency, ...
            rec_diameter, zenith_transmittance, 0,beamwidth_st(w_0[i], ...
            z_0[i], r_0(0, orbit_height, k, hv_5_7_model), 600000., ...
            k),jitter_energy_loss_factor(beamwidth_st(w_0[i], z_0[i], ...
            r_0(0, orbit_height, k, hv_5_7_model), 600000., k), ...
            600000, [sdelay5[i],sant[i],sal[i],ss[i]]))for i in ...
            range(len(dia))]
331
332
333
334         #Plot the individual errors as a function of transmitter diameter
335         plt.plot(dia,sdelay,label="$\sigma_{tilt\, delay}$",lw=3.0)
336         plt.plot(dia,sant,label="$\sigma_{tilt\, ani}$",lw=3.0,ls='--')
337         plt.plot(dia,sal,label="$\sigma_{CA}$",lw=3.0,ls='-.')
338         plt.plot(dia,ss,label="$\sigma_{SNR}$",lw=3.0,ls=':')
339         plt.plot(dia,stot,label="$\sigma_{total}$",lw=3.0)
340         plt.ticklabel_format(style='sci',axis='y',scilimits=(0,0))
341         plt.legend(loc=1)
342
```

```
343         #Plot the total error as a function of transmitter diameter ...
               for different bandwidths
344         #plt.plot(dia,stot1,label="20 Hz",lw=3.0)
345         #plt.plot(dia,stot2,label="40 Hz",lw=3.0,ls='--')
346         #plt.plot(dia,stot3,label="60 Hz",lw=3.0,ls='-.')
347         #plt.plot(dia,stot4,label="80 Hz",lw=3.0,ls=':')
348         #plt.plot(dia,stot5,label="100 Hz",lw=3.0)
349         #plt.xlabel('Transmitter diameter [m]')
350         #plt.ylabel('RMS Residual Tilt [rad]')
351         #plt.ticklabel_format(style='sci',axis='y',scilimits=(0,0))
352         #plt.legend(loc=1)
353
354         #Plot the link efficiency as a function of transmitter ...
               diameter for different bandwidths
355         #plt.plot(dia,linke1,label="20 Hz",lw=3.0)
356         #plt.plot(dia,linke2,label="40 Hz",lw=3.0,ls='--')
357         #plt.plot(dia,linke3,label="60 Hz",lw=3.0,ls='-.')
358         #plt.plot(dia,linke4,label="80 Hz",lw=3.0,ls=':')
359         #plt.plot(dia,linke5,label="100 Hz",lw=3.0)
360         #plt.legend(loc=4)
361         #plt.xlabel('Transmitter diameter [m]')
362         #plt.ylabel('Link efficiency [dB]')
363
364
365         plt.show()
366
367     #Section 3 can be used to calculate and plot the spatial fitting ...
           error strehl ratio as well as its link efficiency for ...
           different transmitter diameters
368     #All calculations are done for zenith in this section
369     if 3 in figures:
370         #The spatial fitting error formula is only a good ...
               approximation when the number of modes corrected is ...
               greater than 10
371         #Zernike mode range for greater than 9 modes
372         dat=range(10,138)
373         #Zernike mode range for first 10 modes
374         dat2=range(1,11)
375
376         #Spatial fitting error for fewer than 11 modes for different ...
               transmitter diameters
377         sfit25_below=[sqrt(1.0299*(0.25/r_0(0, orbit_height, k, ...
               hv_5_7_model))**(5./3.)),sqrt(0.582*(0.25/r_0(0, ...
               orbit_height, k, ...
```

```
            hv_5_7_model))**(5./3.)),sqrt(0.134*(0.25/r_0(0, ...
            orbit_height, k, ...
            hv_5_7_model))**(5./3.)),sqrt(0.111*(0.25/r_0(0, ...
            orbit_height, k, ...
            hv_5_7_model))**(5./3.)),sqrt(0.0880*(0.25/r_0(0, ...
            orbit_height, k, ...
            hv_5_7_model))**(5./3.)),sqrt(0.0648*(0.25/r_0(0, ...
            orbit_height, k, ...
            hv_5_7_model))**(5./3.)),sqrt(0.0587*(0.25/r_0(0, ...
            orbit_height, k, ...
            hv_5_7_model))**(5./3.)),sqrt(0.0525*(0.25/r_0(0, ...
            orbit_height, k, ...
            hv_5_7_model))**(5./3.)),sqrt(0.0463*(0.25/r_0(0, ...
            orbit_height, k, ...
            hv_5_7_model))**(5./3.)),sqrt(0.0401*(0.25/r_0(0, ...
            orbit_height, k, hv_5_7_model))**(5./3.))]
378         sfit50_below=[sqrt(1.0299*(0.5/r_0(0, orbit_height, k, ...
            hv_5_7_model))**(5./3.)),sqrt(0.582*(0.5/r_0(0, ...
            orbit_height, k, ...
            hv_5_7_model))**(5./3.)),sqrt(0.134*(0.5/r_0(0, ...
            orbit_height, k, ...
            hv_5_7_model))**(5./3.)),sqrt(0.111*(0.5/r_0(0, ...
            orbit_height, k, ...
            hv_5_7_model))**(5./3.)),sqrt(0.0880*(0.5/r_0(0, ...
            orbit_height, k, ...
            hv_5_7_model))**(5./3.)),sqrt(0.0648*(0.5/r_0(0, ...
            orbit_height, k, ...
            hv_5_7_model))**(5./3.)),sqrt(0.0587*(0.5/r_0(0, ...
            orbit_height, k, ...
            hv_5_7_model))**(5./3.)),sqrt(0.0525*(0.5/r_0(0, ...
            orbit_height, k, ...
            hv_5_7_model))**(5./3.)),sqrt(0.0463*(0.5/r_0(0, ...
            orbit_height, k, ...
            hv_5_7_model))**(5./3.)),sqrt(0.0401*(0.5/r_0(0, ...
            orbit_height, k, hv_5_7_model))**(5./3.))]
379         sfit75_below=[sqrt(1.0299*(0.75/r_0(0, orbit_height, k, ...
            hv_5_7_model))**(5./3.)),sqrt(0.582*(0.75/r_0(0, ...
            orbit_height, k, ...
            hv_5_7_model))**(5./3.)),sqrt(0.134*(0.75/r_0(0, ...
            orbit_height, k, ...
            hv_5_7_model))**(5./3.)),sqrt(0.111*(0.75/r_0(0, ...
            orbit_height, k, ...
            hv_5_7_model))**(5./3.)),sqrt(0.0880*(0.75/r_0(0, ...
            orbit_height, k, ...
```

```
            hv_5_7_model))**(5./3.)),sqrt(0.0648*(0.75/r_0(0, ...
            orbit_height, k, ...
            hv_5_7_model))**(5./3.)),sqrt(0.0587*(0.75/r_0(0, ...
            orbit_height, k, ...
            hv_5_7_model))**(5./3.)),sqrt(0.0525*(0.75/r_0(0, ...
            orbit_height, k, ...
            hv_5_7_model))**(5./3.)),sqrt(0.0463*(0.75/r_0(0, ...
            orbit_height, k, ...
            hv_5_7_model))**(5./3.)),sqrt(0.0401*(0.75/r_0(0, ...
            orbit_height, k, hv_5_7_model))**(5./3.))]
380         sfit100_below=[sqrt(1.0299*(1./r_0(0, orbit_height, k, ...
            hv_5_7_model))**(5./3.)),sqrt(0.582*(1./r_0(0, ...
            orbit_height, k, ...
            hv_5_7_model))**(5./3.)),sqrt(0.134*(1./r_0(0, ...
            orbit_height, k, ...
            hv_5_7_model))**(5./3.)),sqrt(0.111*(1./r_0(0, ...
            orbit_height, k, ...
            hv_5_7_model))**(5./3.)),sqrt(0.0880*(1./r_0(0, ...
            orbit_height, k, ...
            hv_5_7_model))**(5./3.)),sqrt(0.0648*(1./r_0(0, ...
            orbit_height, k, ...
            hv_5_7_model))**(5./3.)),sqrt(0.0587*(1./r_0(0, ...
            orbit_height, k, ...
            hv_5_7_model))**(5./3.)),sqrt(0.0525*(1./r_0(0, ...
            orbit_height, k, ...
            hv_5_7_model))**(5./3.)),sqrt(0.0463*(1./r_0(0, ...
            orbit_height, k, ...
            hv_5_7_model))**(5./3.)),sqrt(0.0401*(1./r_0(0, ...
            orbit_height, k, hv_5_7_model))**(5./3.))]
381         #Spatial fitting error for greater than 9 modes for different ...
            transmitter diameters
382         sfit25_above = [sigma_fit(0.25, r_0(0, orbit_height, k, ...
            hv_5_7_model), i)for i in dat]
383         sfit50_above = [sigma_fit(0.50, r_0(0, orbit_height, k, ...
            hv_5_7_model), i)for i in dat]
384         sfit75_above = [sigma_fit(0.75, r_0(0, orbit_height, k, ...
            hv_5_7_model), i)for i in dat]
385         sfit100_above = [sigma_fit(1.00, r_0(0, orbit_height, k, ...
            hv_5_7_model), i)for i in dat]
386
387         #Strehl ratio for spatial fitting error with fewer than 11 ...
            modes for different transmitter diameters
388         st25_below=[strehl_approx([sqrt(1.0299*(0.25/r_0(0, ...
            orbit_height, k, hv_5_7_model))**(5./3.))]),
```

```
389             strehl_approx([sqrt(0.582*(0.25/r_0(0, orbit_height, k, ...
                    hv_5_7_model))**(5./3.))]),
390             strehl_approx([sqrt(0.134*(0.25/r_0(0, orbit_height, k, ...
                    hv_5_7_model))**(5./3.))]),
391             strehl_approx([sqrt(0.111*(0.25/r_0(0, orbit_height, k, ...
                    hv_5_7_model))**(5./3.))]),
392             strehl_approx([sqrt(0.0880*(0.25/r_0(0, orbit_height, k, ...
                    hv_5_7_model))**(5./3.))]),
393             strehl_approx([sqrt(0.0648*(0.25/r_0(0, orbit_height, k, ...
                    hv_5_7_model))**(5./3.))]),
394             strehl_approx([sqrt(0.0587*(0.25/r_0(0, orbit_height, k, ...
                    hv_5_7_model))**(5./3.))]),
395             strehl_approx([sqrt(0.0525*(0.25/r_0(0, orbit_height, k, ...
                    hv_5_7_model))**(5./3.))]),
396             strehl_approx([sqrt(0.0463*(0.25/r_0(0, orbit_height, k, ...
                    hv_5_7_model))**(5./3.))]),
397             strehl_approx([sqrt(0.0401*(0.25/r_0(0, orbit_height, k, ...
                    hv_5_7_model))**(5./3.))])]
398         st50_below=[strehl_approx([sqrt(1.0299*(0.5/r_0(0, ...
                orbit_height, k, hv_5_7_model))**(5./3.))]),
399             strehl_approx([sqrt(0.582*(0.5/r_0(0, orbit_height, k, ...
                    hv_5_7_model))**(5./3.))]),
400             strehl_approx([sqrt(0.134*(0.5/r_0(0, orbit_height, k, ...
                    hv_5_7_model))**(5./3.))]),
401             strehl_approx([sqrt(0.111*(0.5/r_0(0, orbit_height, k, ...
                    hv_5_7_model))**(5./3.))]),
402             strehl_approx([sqrt(0.0880*(0.5/r_0(0, orbit_height, k, ...
                    hv_5_7_model))**(5./3.))]),
403             strehl_approx([sqrt(0.0648*(0.5/r_0(0, orbit_height, k, ...
                    hv_5_7_model))**(5./3.))]),
404             strehl_approx([sqrt(0.0587*(0.5/r_0(0, orbit_height, k, ...
                    hv_5_7_model))**(5./3.))]),
405             strehl_approx([sqrt(0.0525*(0.5/r_0(0, orbit_height, k, ...
                    hv_5_7_model))**(5./3.))]),
406             strehl_approx([sqrt(0.0463*(0.5/r_0(0, orbit_height, k, ...
                    hv_5_7_model))**(5./3.))]),
407             strehl_approx([sqrt(0.0401*(0.5/r_0(0, orbit_height, k, ...
                    hv_5_7_model))**(5./3.))])]
408         st75_below=[strehl_approx([sqrt(1.0299*(0.75/r_0(0, ...
                orbit_height, k, hv_5_7_model))**(5./3.))]),
409         strehl_approx([sqrt(0.582*(0.75/r_0(0, orbit_height, k, ...
                hv_5_7_model))**(5./3.))]),
410         strehl_approx([sqrt(0.134*(0.75/r_0(0, orbit_height, k, ...
                hv_5_7_model))**(5./3.))]),
```

```
411         strehl_approx([sqrt(0.111*(0.75/r_0(0, orbit_height, k, ...
                hv_5_7_model))**(5./3.))]),
412         strehl_approx([sqrt(0.0880*(0.75/r_0(0, orbit_height, k, ...
                hv_5_7_model))**(5./3.))]),
413         strehl_approx([sqrt(0.0648*(0.75/r_0(0, orbit_height, k, ...
                hv_5_7_model))**(5./3.))]),
414         strehl_approx([sqrt(0.0587*(0.75/r_0(0, orbit_height, k, ...
                hv_5_7_model))**(5./3.))]),
415         strehl_approx([sqrt(0.0525*(0.75/r_0(0, orbit_height, k, ...
                hv_5_7_model))**(5./3.))]),
416         strehl_approx([sqrt(0.0463*(0.75/r_0(0, orbit_height, k, ...
                hv_5_7_model))**(5./3.))]),
417         strehl_approx([sqrt(0.0401*(0.75/r_0(0, orbit_height, k, ...
                hv_5_7_model))**(5./3.))])]
418         st100_below=[strehl_approx([sqrt(1.0299*(1./r_0(0, ...
                orbit_height, k, hv_5_7_model))**(5./3.))]),
419         strehl_approx([sqrt(0.582*(1./r_0(0, orbit_height, k, ...
                hv_5_7_model))**(5./3.))]),
420         strehl_approx([sqrt(0.134*(1./r_0(0, orbit_height, k, ...
                hv_5_7_model))**(5./3.))]),
421         strehl_approx([sqrt(0.111*(1./r_0(0, orbit_height, k, ...
                hv_5_7_model))**(5./3.))]),
422         strehl_approx([sqrt(0.0880*(1./r_0(0, orbit_height, k, ...
                hv_5_7_model))**(5./3.))]),
423         strehl_approx([sqrt(0.0648*(1./r_0(0, orbit_height, k, ...
                hv_5_7_model))**(5./3.))]),
424         strehl_approx([sqrt(0.0587*(1./r_0(0, orbit_height, k, ...
                hv_5_7_model))**(5./3.))]),
425         strehl_approx([sqrt(0.0525*(1./r_0(0, orbit_height, k, ...
                hv_5_7_model))**(5./3.))]),
426         strehl_approx([sqrt(0.0463*(1./r_0(0, orbit_height, k, ...
                hv_5_7_model))**(5./3.))]),
427         strehl_approx([sqrt(0.0401*(1./r_0(0, orbit_height, k, ...
                hv_5_7_model))**(5./3.))])]
428         #Strehl ratio for spatial fitting error with greater than 9 ...
                modes for different transmitter diameters
429         st25_above=[strehl_approx([sigma_fit(0.25, r_0(0, ...
                orbit_height, k, hv_5_7_model), i)])for i in dat]
430         st50_above=[strehl_approx([sigma_fit(0.5, r_0(0, ...
                orbit_height, k, hv_5_7_model), i)])for i in dat]
431         st75_above=[strehl_approx([sigma_fit(0.75, r_0(0, ...
                orbit_height, k, hv_5_7_model), i)])for i in dat]
432         st100_above=[strehl_approx([sigma_fit(1, r_0(0, orbit_height, ...
                k, hv_5_7_model), i)])for i in dat]
```

```
433
434         #Link efficiencies incorporating the spatial fitting error as ...
               a function of number of Zernike modes corrected for ...
               different transmitter diameters
435         #(test1 through test4 are for modes>9, test5 through test8 ...
               are for modes<11
436         w_0 = 1./sqrt(2*log(2))*0.25/2.
437         z_0 = pi*w_0**2/wavelength
438         linke25_above=[link_efficiency_ao(trans_efficiency, ...
               rec_efficiency, rec_diameter, zenith_transmittance, 0, ...
               beamwidth_diff(w_0, z_0, orbit_height),1., ...
               beamwidth_st(w_0, z_0, r_0(0, orbit_height, k, ...
               hv_5_7_model),orbit_height, k),1., [sfit25_above[i]])for i ...
               in range(len(dat))]
439         w_0 = 1./sqrt(2*log(2))*0.5/2.
440         z_0 = pi*w_0**2/wavelength
441         linke50_above=[link_efficiency_ao(trans_efficiency, ...
               rec_efficiency, rec_diameter, zenith_transmittance, 0, ...
               beamwidth_diff(w_0, z_0, orbit_height),1., ...
               beamwidth_st(w_0, z_0, r_0(0, orbit_height, k, ...
               hv_5_7_model),orbit_height, k),1., [sfit50_above[i]])for i ...
               in range(len(dat))]
442         w_0 = 1./sqrt(2*log(2))*0.75/2.
443         z_0 = pi*w_0**2/wavelength
444         linke75_above=[link_efficiency_ao(trans_efficiency, ...
               rec_efficiency, rec_diameter, zenith_transmittance, 0, ...
               beamwidth_diff(w_0, z_0, orbit_height),1., ...
               beamwidth_st(w_0, z_0, r_0(0, orbit_height, k, ...
               hv_5_7_model),orbit_height, k),1., [sfit75_above[i]])for i ...
               in range(len(dat))]
445         w_0 = 1./sqrt(2*log(2))*1.0/2.
446         z_0 = pi*w_0**2/wavelength
447         linke100_above=[link_efficiency_ao(trans_efficiency, ...
               rec_efficiency, rec_diameter, zenith_transmittance, 0, ...
               beamwidth_diff(w_0, z_0, orbit_height),1., ...
               beamwidth_st(w_0, z_0, r_0(0, orbit_height, k, ...
               hv_5_7_model),orbit_height, k),1., [sfit100_above[i]])for ...
               i in range(len(dat))]
448         w_0 = 1./sqrt(2*log(2))*0.25/2.
449         z_0 = pi*w_0**2/wavelength
450         linke25_below=[link_efficiency_ao(trans_efficiency, ...
               rec_efficiency, rec_diameter, zenith_transmittance, 0, ...
               beamwidth_diff(w_0, z_0, orbit_height),1., ...
               beamwidth_st(w_0, z_0, r_0(0, orbit_height, k, ...
```

```
            hv_5_7_model),orbit_height, k),1., [sfit25_below[i]])for i ...
            in range(len(dat2))]
451         w_0 = 1./sqrt(2*log(2))*0.5/2.
452         z_0 = pi*w_0**2/wavelength
453         linke50_below=[link_efficiency_ao(trans_efficiency, ...
            rec_efficiency, rec_diameter, zenith_transmittance, 0, ...
            beamwidth_diff(w_0, z_0, orbit_height),1., ...
            beamwidth_st(w_0, z_0, r_0(0, orbit_height, k, ...
            hv_5_7_model),orbit_height, k),1., [sfit50_below[i]])for i ...
            in range(len(dat2))]
454         w_0 = 1./sqrt(2*log(2))*0.75/2.
455         z_0 = pi*w_0**2/wavelength
456         linke75_below=[link_efficiency_ao(trans_efficiency, ...
            rec_efficiency, rec_diameter, zenith_transmittance, 0, ...
            beamwidth_diff(w_0, z_0, orbit_height),1., ...
            beamwidth_st(w_0, z_0, r_0(0, orbit_height, k, ...
            hv_5_7_model),orbit_height, k),1., [sfit75_below[i]])for i ...
            in range(len(dat2))]
457         w_0 = 1./sqrt(2*log(2))*1.0/2.
458         z_0 = pi*w_0**2/wavelength
459         linke100_below=[link_efficiency_ao(trans_efficiency, ...
            rec_efficiency, rec_diameter, zenith_transmittance, 0, ...
            beamwidth_diff(w_0, z_0, orbit_height),1., ...
            beamwidth_st(w_0, z_0, r_0(0, orbit_height, k, ...
            hv_5_7_model),orbit_height, k),1., [sfit100_below[i]])for ...
            i in range(len(dat2))]
460
461         #Plot the strehl ratio for the spatial fitting error as a ...
            function of number of modes corrected for different ...
            transmitter diameters
462         plt.plot(dat2,st25_below,lw=3.0,color='b')
463         plt.plot(dat2,st50_below,lw=3.0,color='r',ls='--')
464         plt.plot(dat2,st75_below,lw=3.0,color='g',ls='-.')
465         plt.plot(dat2,st100_below,lw=3.0,color='m',ls=':')
466         plt.plot(dat,st25_above,label="D = 0.25 m",lw=3.0,color='b')
467         plt.plot(dat,st50_above,label="D = 0.50 ...
            m",lw=3.0,color='r',ls='--')
468         plt.plot(dat,st75_above,label="D = 0.75 ...
            m",lw=3.0,color='g',ls='-.')
469         plt.plot(dat,st100_above,label="D = 1.00 ...
            m",lw=3.0,color='m',ls=':')
470         plt.legend(loc=4)
471         plt.xlabel('N modes corrected')
472         plt.ylabel('Strehl')
```

```
473
474         #Plot the link efficiency for the spatial fitting error as a ...
                function of number of modes corrected for different ...
                transmitter diameters
475         #plt.plot(dat,linke25_above,label="D = 0.25 m",lw=3.0,color='b')
476         #plt.plot(dat,linke50_above,label="D = 0.50 ...
                m",lw=3.0,color='r',ls='--')
477         #plt.plot(dat,linke75_above,label="D = 0.75 ...
                m",lw=3.0,color='g',ls='-.')
478         #plt.plot(dat,linke100_above,label="D = 1.00 ...
                m",lw=3.0,color='m',ls=':')
479         #plt.plot(dat2,linke25_below,lw=3.0,color='b')
480         #plt.plot(dat2,linke50_below,lw=3.0,color='r',ls='--')
481         #plt.plot(dat2,linke75_below,lw=3.0,color='g',ls='-.')
482         #plt.plot(dat2,linke100_below,lw=3.0,color='m',ls=':')
483         #plt.legend(loc=4)
484         #plt.xlabel('N modes corrected')
485         #plt.ylabel('Link efficiency [dB]')
486
487         plt.show()
488
489     #Section 4 can be used to calculate and plot total effect of AO ...
            on link efficiency as a function of elevation angle
490     if 4 in figures:
491         #Angle from zenith
492         iss = range(0, 81)
493         #Elevation angle
494         elev=range(90,9,-1)
495         #Atmospheric model
496         atm_model=hv_5_7_model
497         #Laser guide star height
498         LGS_height = 18000.
499         #Fried's parameters as a function of angle from zenith
500         r0s = [r_0(i*pi/180, orbit_height, k, atm_model) for i in iss]
501         #Tip/tilt delay error as a function of angle from zenith
502         sdelay=[sigma_wander_delay(wavelength, trans_diameter, ...
                    loop_bandwidth, i*pi/180, orbit_height, atm_model, ...
                    bufton_wind, wind_speed)for i in iss]
503         #Tip/tilt anisoplanatism error as a function of angle from zenith
504         sant = [sigma_ani_tilt(trans_diameter, ...
                    sat_angular_sweep(i*pi/180, orbit_height, earth_radius, ...
                    earth_mass), i*pi/180, orbit_height, atm_model) for i in iss]
505         #Tip/tilt centroid anisoplanatism error as a function of ...
                angle from zenith
```

```
506         sal = [sigma_alias(wavelength, trans_diameter, r0s[i]) for i ...
                in iss]
507         #Signal to noise sensor error
508         ss = [sigma_snr for i in iss]
509         #Distance from satellite to ground station as a function of ...
                angle from zenith
510         dists = [sat_dist_from_zenith(i*pi/180, orbit_height, ...
                earth_radius) for i in iss]
511         #Phase delay error as a function of angle from zenith
512         sad = [sigma_ao_delay(wavelength, loop_bandwidth, i*pi/180, ...
                orbit_height, atm_model, bufton_wind, wind_speed)for i in iss]
513         #Spatial fitting error as a function of angle from zenith
514         sfit = [sigma_fit(trans_diameter, r0s[i], zernike_modes)for i ...
                in iss]
515         #Phase anisoplanatism error as a function of angle from zenith
516         sanp = [sigma_ani_phase(k, i*pi/180, orbit_height, ...
                earth_radius, earth_mass, atm_model)for i in iss]
517         #LGS cone error as a function of angle from zenith
518         scone = [sigma_cone(trans_diameter, wavelength, orbit_height, ...
                i*pi/180, LGS_height, atm_model)for i in iss]
519
520         #Link efficiency for diffraciton limited beam (S=1,I=1)
521         DiffracLimit=[link_efficiency_ao(trans_efficiency, ...
                rec_efficiency, rec_diameter, zenith_transmittance, ...
                (i)*pi/180, beamwidth_diff(w_0, z_0, dists[i]), 1., ...
                beamwidth_diff(w_0, z_0, dists[i]), 1., [])for i in ...
                range(len(iss))]
522         #Link efficiency for perfect phase correction and system ...
                limited tip/tilt correction (S=1,I<1)
523         AOCorrectionOnlyTilt=[link_efficiency_ao(trans_efficiency, ...
                rec_efficiency, rec_diameter, zenith_transmittance, ...
                (i)*pi/180, beamwidth_diff(w_0, z_0, dists[i]), ...
                jitter_energy_loss_factor(beamwidth_diff(w_0, z_0, ...
                dists[i]), dists[i], [sdelay[i],sant[i],ss[i],sal[i]]), ...
                beamwidth_st(w_0, z_0, r0s[i],dists[i], k), ...
                jitter_energy_loss_factor(beamwidth_st(w_0, z_0, ...
                r0s[i],dists[i], k), dists[i], ...
                [sdelay[i],sant[i],ss[i],sal[i]]), [0])for i in ...
                range(len(iss))]
524         #Link efficiency for no phase anisoplanatism, but system ...
                limited phase and tip/tilt correction (S<1,I<1,sanp=0)
525         AOCorrectionNoANP=[link_efficiency_ao(trans_efficiency, ...
                rec_efficiency, rec_diameter, zenith_transmittance, ...
                (i)*pi/180, beamwidth_diff(w_0, z_0, dists[i]), ...
```

```
        jitter_energy_loss_factor(beamwidth_diff(w_0, z_0, ...
        dists[i]), dists[i], [sdelay[i],ss[i],sant[i],sal[i]]), ...
        beamwidth_st(w_0, z_0, r0s[i],dists[i], k), ...
        jitter_energy_loss_factor(beamwidth_st(w_0, z_0, ...
        r0s[i],dists[i], k), dists[i], ...
        [sdelay[i],ss[i],sal[i],sant[i]]), [sad[i],sfit[i]])for i ...
        in range(len(iss))]
526     #Link efficency for equation which does not take phase errors ...
        into account
527     CorrectTiltOnly=[link_efficiency(trans_efficiency, ...
        rec_efficiency, rec_diameter, zenith_transmittance, ...
        (i)*pi/180, beamwidth_st(w_0, z_0, r0s[i],dists[i], k), ...
        jitter_energy_loss_factor(beamwidth_st(w_0, z_0, ...
        r0s[i],dists[i], k), dists[i], ...
        [sdelay[i],sant[i],sal[i],ss[i]]))for i in range(len(iss))]
528     #Link efficiency for total system limited AO correction (S<1,I<1)
529     AOCorrection=[link_efficiency_ao(trans_efficiency, ...
        rec_efficiency, rec_diameter, zenith_transmittance, ...
        (i)*pi/180, beamwidth_diff(w_0, z_0, dists[i]), ...
        jitter_energy_loss_factor(beamwidth_diff(w_0, z_0, ...
        dists[i]), dists[i], [sdelay[i],sant[i],sal[i],ss[i]]), ...
        beamwidth_st(w_0, z_0, r0s[i],dists[i], k), ...
        jitter_energy_loss_factor(beamwidth_st(w_0, z_0, ...
        r0s[i],dists[i], k), dists[i], ...
        [sdelay[i],sant[i],sal[i],ss[i]]), ...
        [sad[i],sfit[i],sanp[i]])for i in range(len(iss))]
530     #Link efficiency when using a laser guide star
531     AOLGS=[link_efficiency_ao(trans_efficiency, rec_efficiency, ...
        rec_diameter, zenith_transmittance, i*pi/180, ...
        beamwidth_diff(w_0, z_0, dists[i]), ...
        jitter_energy_loss_factor(beamwidth_diff(w_0, z_0, ...
        dists[i]), dists[i], [sdelay[i],sant[i],sal[i],ss[i]]), ...
        beamwidth_st(w_0, z_0, r0s[i],dists[i], k), ...
        jitter_energy_loss_factor(beamwidth_st(w_0, z_0, ...
        r0s[i],dists[i], k), dists[i], ...
        [sdelay[i],sant[i],sal[i],ss[i]]), ...
        [sad[i],sfit[i],scone[i]])for i in iss]
532
533     #Plot the link efficiencies as described above
534     plt.plot(elev,DiffracLimit,label="Diffraction ...
        Limit",lw=3.0,c='black')
535     plt.plot(elev,AOCorrection,label="Full Tilt and Phase ...
        Correction (S<1,I<1)",lw=3.0,c='cyan')
```

```
536         #plt.plot(elev,AOLGS,label="Full Tilt and Phase Correction ...
                with LGS (S<1,I<1)",lw=3.0,c='cyan')
537         plt.plot(elev,AOCorrectionOnlyTilt,label="Perfect Phase ...
                Correction (S=1,I<1)",lw=3.0,color='m',ls='-.')
538         plt.plot(elev,AOCorrectionNoANP,label="No Phase ...
                Anisoplanatism Error ($\sigma_{phase\,ani}=0$, ...
                S<1,I<1)",lw=3.0,color='green',ls=':')
539         plt.plot(elev,CorrectTiltOnly,label="Only Tilt Correction ...
                (S=0,I<1)",lw=3.0,color='r',ls='--')
540         plt.xlabel('Elevation [$^\circ$]')
541         plt.ylabel('Link Efficiency [dB]')
542         plt.legend(loc=4,prop={'size':12})
543         plt.show()
544
545     #Section 5 can be used to calculate and plot the structure ...
            function Cn2 as a function of height
546     if 5 in figures:
547         #Height array
548         h=range(1,25000)
549         #Structure function for the four selected atmospheric models
550         HV57C=[log(csq(i,**hv_5_7_model),10)for i in h]
551         HV1010C=[log(csq(i,**hv_10_10_model),10)for i in h]
552         HV1512C=[log(csq(i,**hv_15_12_model),10)for i in h]
553         TenerifeC=[log(csq(i,**tenerife_model),10)for i in h]
554
555         #Plot the structure functions as a function of height
556         plt.plot(HV57C,h,label="HV 5-7",lw=2)
557         plt.plot(HV1010C,h,label="HV 10-10",lw=2,ls='--')
558         plt.plot(HV1512C,h,label="HV 15-12",lw=2,ls='-.')
559         plt.plot(TenerifeC,h,label="Tenerife",lw=2,ls=':')
560         plt.xlabel("$\log_{10}(C_n^2)$")
561         plt.ylabel("Altitude [m]")
562         plt.legend(loc=1)
563         plt.show()
564
565     #Section 6 can be used to calculate and plot the Bufton wind ...
            model as a function of height
566     if 6 in figures:
567         #Height array
568         h=range(1,25000)
569         #Wind speeds for the 2 selected wind profiles
570         Bufton20=[bufton_wind(i,20)for i in h]
571         Bufton30=[bufton_wind(i,30)for i in h]
572
```

```
573         #Plot the wind speeds as a function of height
574         plt.plot(Bufton20,h,label="$v_t=20$ m/s",lw=2)
575         plt.plot(Bufton30,h,label="$v_t=30$ m/s",lw=2,ls='--')
576         plt.xlabel("$v_w$ [m/s]")
577         plt.ylabel("Altitude [m]")
578         plt.legend(loc=1)
579         plt.show()
```

Appendix B

Waypoint Calculators

QKD airborne trials

Calculate Ground Waypoints for Circular Tracks: 106-246 Make sure to enable VBA Macros!

Set these parameters:

lateral distance [NM]	2.7	NM
bearing from GS to start of arc [deg]	260	Deg
arc angle	-140	deg

5.0004 km
4.537856055 radians
-2.443460953 radians

Arc Step	Angle on arc [deg]	X [km]	Y [km]	X_rot [km]	Y_rot [km]	dLat [rad]	dlong [rad]	lat [decimal deg]	long [decimal deg]	lat [DDMMSS	long [DDMMSS.SS]
0	0.0	5.0	0.000	-0.9	-4.9	-1.36E-04	-1.09E-03	4.4937159E+01	-7.6006437E+01	445613.8	-760023.2
1	-17.5	4.8	-1.504	-2.3	-4.4	-3.63E-04	-9.84E-04	4.4924196E+01	-7.6000220E+01	445527.1	-760000.8
2	-35.0	4.1	-2.868	-3.5	-3.5	-5.55E-04	-7.85E-04	4.4913157E+01	-7.5988784E+01	445447.4	-755919.6
3	-52.5	3.0	-3.967	-4.4	-2.3	-6.97E-04	-5.12E-04	4.4905062E+01	-7.5973186E+01	445418.2	-755823.5
4	-70.0	1.7	-4.699	-4.9	-0.9	-7.73E-04	-1.93E-04	4.4900662E+01	-7.5954872E+01	445402.4	-755717.5
5	-87.5	0.2	-4.996	-5.0	0.7	-7.79E-04	1.45E-04	4.4900364E+01	-7.5935536E+01	445401.3	-755607.9
6	-105.0	-1.3	-4.830	-4.5	2.1	-7.12E-04	4.69E-04	4.4904194E+01	-7.5916968E+01	445415.1	-755501.1
7	-122.5	-2.7	-4.217	-3.7	3.4	-5.79E-04	7.50E-04	4.4911799E+01	-7.5900886E+01	445442.5	-755403.2
8	-140.0	-3.8	-3.214	-2.5	4.3	-3.93E-04	9.61E-04	4.4922475E+01	-7.5888780E+01	445520.9	-755319.6

Results:

iFlightplanner string: - past into: https://www.iflightplanner.com/AviationCharts/

445613.8/-760023.2 445527.1/-760000.8 445447.4/-755919.6 445418.2/-755823.5 445402.4/-755717.5 445401.3/-755607.9 445415.1/-755501.1 445442.5/-755403.2 445520.9/-755319.6

List of Waypoints:

Bearing True [deg	lateral distance [NM]	lat [Degrees]	long [Degrees]	lat [decimal deg]	long [decimal deg]
260.0	2.7	44°56.23	-76°0.386	4.4937159E+01	-7.6006437E+01
242.5	2.7	44°55.452	-76°0.013	4.4924196E+01	-7.6000220E+01
225.0	2.7	44°54.789	-75°59.327	4.4913157E+01	-7.5988784E+01
207.5	2.7	44°54.304	-75°58.391	4.4905062E+01	-7.5973186E+01
190.0	2.7	44°54.04	-75°57.292	4.4900662E+01	-7.5954872E+01
172.5	2.7	44°54.022	-75°56.132	4.4900364E+01	-7.5935536E+01
155.0	2.7	44°54.252	-75°55.018	4.4904194E+01	-7.5916968E+01
137.5	2.7	44°54.708	-75°54.053	4.4911799E+01	-7.5900886E+01
120.0	2.7	44°55.349	-75°53.327	4.4922475E+01	-7.5888780E+01

QKD airborne trials

Calculate Ground Waypoints for Straight Tracks:

Simplistic Waypoint calculations; **we assume flat Euclidian space!**

Make sure to enable VBA Macros!

conversions 0.304800000 m/foot
0.514400000 m/s per KN
1.852000000 km/NM
0.000164579 NM/foot

Earth Radius at Lat 6367.61 km
https://rechneronline.de/earth-radius/

Set these parameters:

		DDDMMSSS		Decimal Degrees	Check
Ground site location (GS)	lat=	44° 56' 41.9"		44.94497222	44°56'41.9
	long=	-75° 56' 37.8"		-75.94383333	-75°57'22.2
minimal lateral distance [NM]			5.4 NM	10.0008 km	
bearing from GS to minimal lateral distance [deg]			150 Deg	2.617993878 radians	

Bearing offset [deg]	X [km]	Y [km]	X_rot [km]	Y_rot [km]	dLat [rad]	dlong [rad]	lat [decimal deg]	long [decimal deg]	lat [DDMMSS.SS]	long [DDMMSS.SS]
46	10.0	10.356	-13.8	-4.0	-2.17E-03	-8.80E-04	4.4820449E+01	-7.5994282E+01	444913.6	-755939.4
40	10.0	8.392	-12.9	-2.3	-2.02E-03	-5.03E-04	4.4829287E+01	-7.5972653E+01	444945.4	-755821.6
20	10.0	3.640	-10.5	1.8	-1.65E-03	4.10E-04	4.4850665E+01	-7.5920339E+01	445102.4	-755513.2
0	10.0	0.000	-8.7	5.0	-1.36E-03	1.11E-03	4.4867041E+01	-7.5880264E+01	445201.3	-755248.9
-20	10.0	-3.640	-6.8	8.2	-1.07E-03	1.81E-03	4.4883417E+01	-7.5840189E+01	445300.3	-755024.7
-40	10.0	-8.392	-4.5	12.3	-7.01E-04	2.72E-03	4.4904795E+01	-7.5787874E+01	445417.3	-754716.3
-46	10.0	-10.356	-3.5	14.0	-5.47E-04	3.10E-03	4.4913633E+01	-7.5766246E+01	445449.1	-754558.5

Results:

iFlightplanner string: - past into: https://www.iflightplanner.com/AviationCharts/

444913.6/-755939.4 444945.4/-755821.6 445102.4/-755513.2 445201.3/-755248.9 445300.3/-755024.7 445417.3/-754716.3 445449.1/-754558.5

Bearing true [deg]	lateral distance [NM]	lat [DDM]	long [DDM]	lat [deg]	long [deg]
196	7.8	44°49.227	-75°59.657	44.82044873	-75.99428157
190	7.0	44°49.757	-75°58.359	44.82928686	-75.97265343
170	5.7	44°51.04	-75°55.22	44.85066465	-75.92033897
150	5.4	44°52.022	-75°52.816	44.86704099	-75.88026377
130	5.7	44°53.005	-75°50.411	44.88341733	-75.84018857
110	7.0	44°54.288	-75°47.272	44.90479512	-75.78787411
104	7.8	44°54.818	-75°45.975	44.91363324	-75.76624597

Appendix C

Selected Photos of Airborne Experiment

Figure C.1: Testing the WiFi at the Brampton Airport. The WiFi antenna was placed in the back of the truck and rotated to follow the airplane as it flew past. It was very cold and we had to switch WiFi rotators part way through the experiment. An incoming snowstorm halted further distance testing as we could no longer see the airplane and the air was becoming too turbulent for comfortable flight.

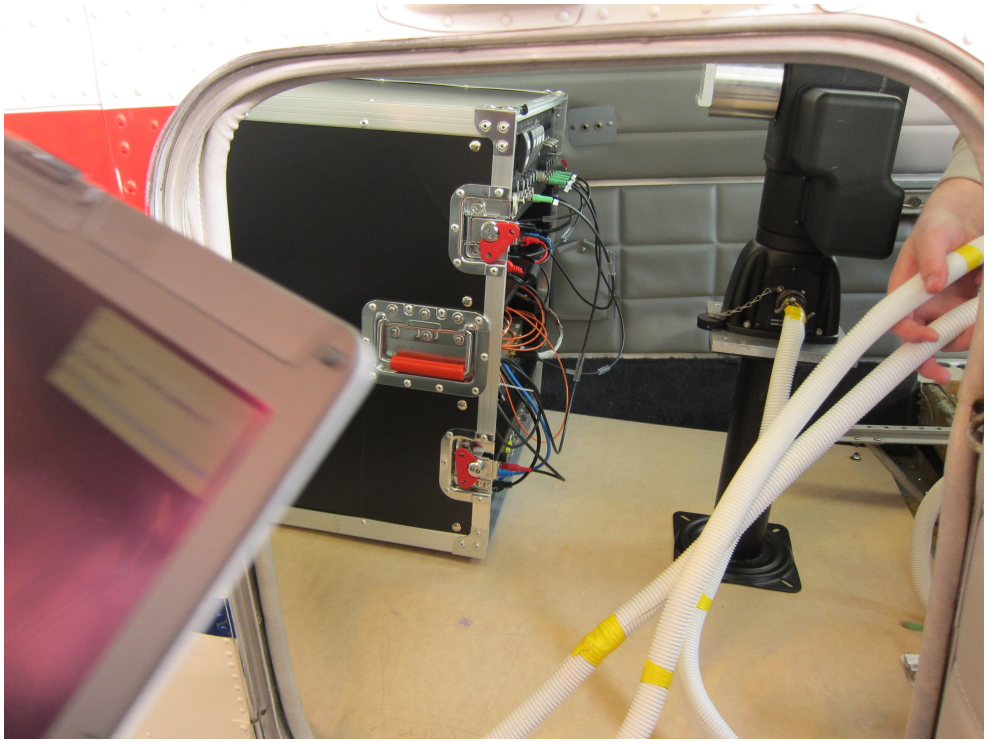


Figure C.2: Fitting the QKD receiver equipment into the Beechcraft Bonanza airplane before the NRC Twin Otter was an option. The small baggage door, as well as the width of the airplane, restricted the range of movement of the telescope limiting usefulness for line passes.

Figure C.3: Carrying case for the QKD receiver telescope, FPU and IOA. We lined a golf club hard travel case with foam to secure the receiver in place when the lid was closed. The case had wheels which allowed for easy transport.

Figure C.4: Sign in front of the NRC Flight Research Laboratory with the logo on the wall in the background in Ottawa, ON.

Figure C.5: Fitting the replica receiver telescope and FLIR mount into the Bell 206 helicopter to check ranges of motion. The angular range of the telescope was limited because the back of the telescope came into contact with the back door.

Figure C.6: Receiver equipment loaded onto a cart and taken to a municipal park approximately 3 km from RAC. The unit was self contained as it had its own power supply and distributor. A successful quantum link was achieved this night.

Figure C.7: The IQC trailer was loaded with all of the equipment for the receiver and transmitter and driven from Waterloo to Smiths Falls to be setup for the ground station.

Figure C.8: The IQC trailer setup at the Smiths Falls–Montague Airport along with the generator and tent to protect the transmitter from the elements when the experiment was not in session.

Figure C.9: The calibration telescope at the ground station used to make sure the bacons and quantum signal were collinear. The telescope was setup ≈20 m away and a visible laser was sent from the transmitter and one beacon at a time for alignment.

Figure C.10: Fog covers the ground station which was common during the first week during the setup of the OGS.

Figure C.11: Dew forming on the transmitter telescope on Monday September 19th, 2016, the day before the first flight.

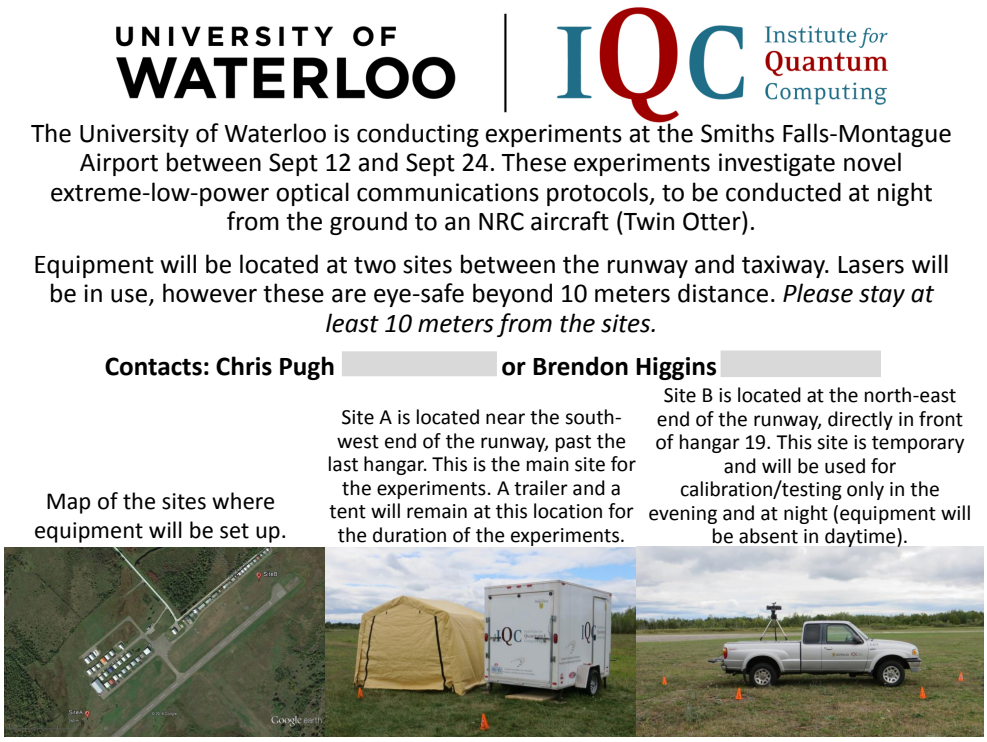


Figure C.12: Information flyer placed in the Smiths Falls Flying Club office to inform the members of our presence and what we were trying to accomplish.

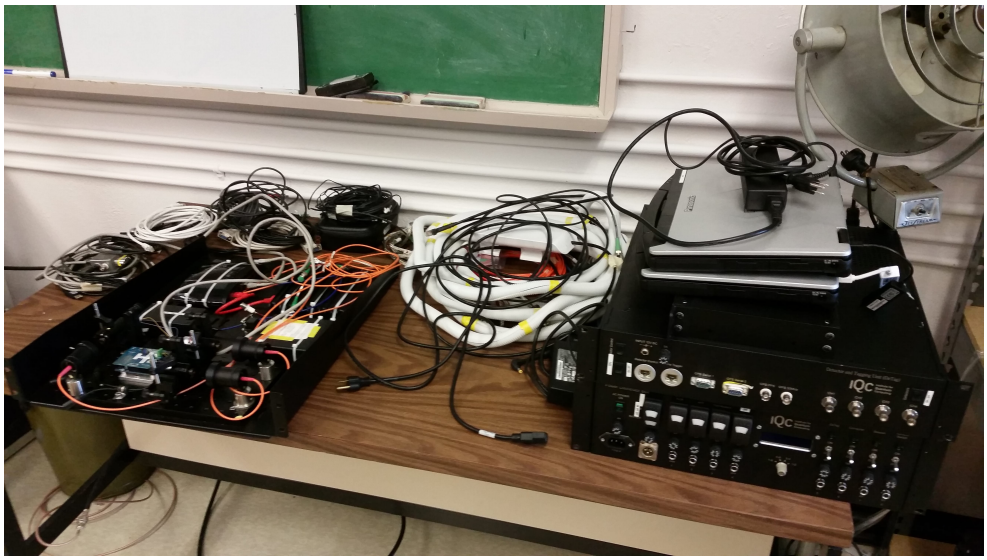


Figure C.13: Preparing the electronics equipment to be mounted into the airplane. Each piece had to be certified as airworthy and minor modifications such as TyRaps, Velcro, and lock tight were made.

Figure C.14: Preparing the cabin of the airplane to install the QKD receiver telescope and electronics. The port in the bottom of the plane normally holds a camera for other experiments but was closed for our flights.

Figure C.15: Airplane being fueled and prepared for the daytime flight.

Figure C.16: Getting ready for the daytime flight. We had harnesses which connected us to the floor and allowed me to reach the equipment, while not being able to exit the open door.

Figure C.17: Image of the ground through the open side door just after take-off.

Figure C.18: Smiths Falls–Montague Airport as seen from the airplane through the open side door. The telescope can be seen in the extreme left of the image.

Figure C.19: The OGS at night during one of the flight trials. The airplane can be seen as the white streak in the sky.

Figure C.20: The IQC and NRC teams in front of the Twin Otter airplane after successfully demonstrating Quantum Key Distribution to a moving aircraft.

Figure C.21: Christopher Pugh and Thomas Jennewein beside stickers from other flight campaigns pointing at the IQC/UW sticker on the Twin Otter airplane.

Appendix D

Publications and Media Attention

D.1 Publications during PhD, 2013–2017

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

- **C. J. Pugh**, P. Kolenderski, C. Scarcella, A. Tosi, T. Jennewein, "Towards correcting atmospheric beam wander via pump beam control in a down conversion process," *Optics Express 24, 18, 20947-20955*, 2016

- J.-P. Bourgoin, B. L. Higgins, N. Gigov, C. Holloway, **C. J. Pugh**, S. Kaiser, M. Cranmer, T. Jennewein, "Free-space quantum key distribution to a moving receiver," *Optics Express 23, 26, 33437-33447*, 2015

D.2 Conference Proceedings

- T. Jennewein, C. Grant, E. Choi, **C. Pugh**, C. Holloway, J.-P. Bourgoin, H. Hakima, B. Higgins, R. Zee, "The NanoQEY mission: ground to space quantum key and entanglement distribution using a nanosatellite," *SPIE Security + Defence, 925402-925402-6*, 2014

D.3 Manuscripts in Preparation

- **C. J. Pugh**, S. Kaiser, J.-P. Bourgoin, B. L. Higgins, S. Turbide, G. Anctil, P. Côté, M. Wang, M. Otis, L. Martin, L. Gagnon, R. Cooney, E. Choi, T. Jennewein, "A fine pointing system suitable for quantum communications on a satellite," *in preparation*
- **C. J. Pugh**, J.-F. Lavigne, J.-P. Bourgoin, B. L. Higgins, T. Jennewein, "Adaptive optics for quantum key distribution between an Earth station and a satellite," *in preparation*

D.4 Media Coverage

- Also featured in: *Primeur Magazine, PhysicsWorld, Scientific Computing, Space Daily, Health Medicinet, Science Newsline, ECN, Science Daily, and EurekAlert!.*
- "Study proves viability of quantum satellite communications," *Phys.org*, June 6, 2017
- I. Froese, "Pugh taking quantum leap," *Brandon Sun*, Print p1, April 25, 2017
- S. Chen, "Physicists, Lasers, and an Airplane: Taking Aim at Quantum Cryptography," *Wired*, Feb 2, 2017
- "CAP Member Chris Pugh featured in Globe and Mail," *cap.ca*, Dec 23, 2016
- G. Mercer, "Waterloo team pulls off encryption breakthrough," *Waterloo Record*, p1-2, Dec 22, 2017
- "We've got photons!", *Institute for Quantum Computing News*, Dec 22, 2016
- I. Semeniuk, "Canadians solve key puzzle for future of encryption," *The Globe and Mail*, Online Dec 20, 2016, Print p1 and A14, Dec 21, 2017
- "Researchers successfully demonstrate prototype for space-based quantum-secured communication", *Institute for Quantum Computing News*, Dec 21, 2016
- "IQC Researchers Successfully Conduct Airborne Demonstration of Quantum Key Distribution," *CASI Toronto Flyer*, p5-6, Nov 2016
- "IQC researchers successfully conduct airborne demonstration of quantum key distribution," *Institute for Quantum Computing News*, Oct 12, 2016