Enabling Technologies for High-Rate, Free-Space Quantum Communication

by

Clinton T. Cahall

Department of Electrical and Computer Engineering
Duke University

Date: _____

Approved:

_____
Jungsang Kim, Supervisor

_____
Martin A. Brooke

_____
Daniel J. Gauthier

_____
Hisham Z. Massoud

_____
Aaron J. Miller

Dissertation submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy in the Department of Electrical and Computer Engineering in the Graduate School of Duke University
2019

Abstract

Enabling Technologies for High-Rate, Free-Space Quantum Communication

by

Clinton T. Cahall

Department of Electrical and Computer Engineering
Duke University

Date: _____

Approved:

_____
Jungsang Kim, Supervisor

_____
Martin A. Brooke

_____
Daniel J. Gauthier

_____
Hisham Z. Massoud

_____
Aaron J. Miller

An abstract of a dissertation submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy in the Department of Electrical and Computer Engineering
in the Graduate School of Duke University
2019

Copyright © 2019 by Clinton T. Cahall
All rights reserved except the rights granted by the
Creative Commons Attribution-Noncommercial Licence

Abstract

Quantum communication protocols, such as quantum key distribution (QKD), are practically important in the dawning of a new quantum information age where quantum computers can perform efficient prime factorization to render public key cryptosystems obsolete. QKD is a communication scheme that utilizes the quantum state of a single photons to transmit information, such as a cryptographic key, that is robust against adversaries including those with a quantum computer. In this thesis I describe the contributions that I have made to the development of high-rate, free-space quantum communication systems.

My effort is focused on building a robust quantum receiver for a high-dimensional time-phase QKD protocol where the data is encoded and secured using a single photon's timing and phase degrees of freedom. This type of communication protocol can encode information in a high-dimensional state, allowing the transmission of > 1 bit per photon. To realize a successful implementation of the protocol a high-performance single-photon detection system must be constructed. My contribution to the field begins with the development of low-noise, low-power cryogenic amplifiers for a detection system using superconducting nanowire single-photon detectors (SNSPDs). Detector characteristics such as maximum count rate and timing resolution are heavily influenced by the design of the read-out circuits that sense and amplify the detection signal. I demonstrate a read-out system with a maximum count rate $>$ 20 million counts-per-second and timing resolution as high as 35 ps.

These results are achieved while maintaining a low power dissipation $< 3\,\mathrm{mW}$ at $4\,\mathrm{K}$ operation, enabling a scalable read-out circuit strategy.

A second contribution I make to the development of detection systems utilizing SNSPDs is extending the superb performance of these detectors to include photon number resolving capabilities. I demonstrate that SNSPDs exhibit multi-photon detection up to four photons where the absorbed photo number is encoded in the rise time of the electrical waveform generated by the detector. Additionally, our experiment agrees well with the predictions of a universal model for turn-on dynamics of SNSPDs. A feature our multi-photon detection system demonstrates high resolution between $n = 1$ and $n > 1$ photons with a bit-error-rate (BER) of 4.2×10^{-4}.

Finally, I extend the utility of the time-phase QKD protocol to free-space applications. Atmospheric turbulences cause spatial mode scrambling of the optical beam during transmission. Therefore, the quantum receiver, and most importantly the time-delay interferometer needed for the measurement of a phase encoding of a single photon, must support many spatial modes. I construct and characterize an interferometer with a $5\,\mathrm{GHz}$ free spectral range that has a wide field-of-view and is passively a-thermal. The results of interferometer characterization are highlighted by a $> 99\,\%$ single-mode, and $> 98\,\%$ multi-mode interference visibility with negligible dependence on the spatial mode structure of the input beam and modest temperature fluctuations. Additionally, the interferometer displays a small path-length shift of $130\,\mathrm{nm}/^{\circ}\mathrm{C}$, allowing for great thermal stability with modest temperature control.

To my wife, my brother, and my parents

Contents

Abstract **iv**

List of Figures **x**

List of Abbreviations and Symbols **xiii**

Acknowledgements **xvi**

1 Introduction **1**

1.1 Secure Communication 2

1.1.1 Public Key Cryptography 3

1.1.2 Private Key Cryptography 4

1.2 Quantum Communication Systems 5

1.3 Thesis and Contribution Overview 6

2 Quantum Communication **9**

2.1 Quantum Foundations 9

2.2 Quantum Key Distribution 10

2.2.1 BB84 11

2.3 Security of QKD 13

2.3.1 Individual Attacks 14

2.3.2 Collective Attacks 15

2.3.3 Coherent Attacks 15

2.3.4 Side-Channel Attacks 15

2.4 Time-Phase QKD . . . 16
2.4.1 $d = 2$ Time-Phase . . . 17
2.4.2 $d = 4$ Time-Phase . . . 21
2.5 Conclusion . . . 23
3 Receiver Infrastructure **25**
3.1 Cryostat . . . 26
3.2 Electrical and Optical Access . . . 29
3.3 Superconducting Nanowire Single-Photon Detectors . . . 31
3.4 Conclusion . . . 34
4 Cryogenic Amplifiers **35**
4.1 SiGe Op-Amp Read-out . . . 37
4.2 GaAs MMIC Read-out . . . 40
4.3 Maximum Count Rate . . . 44
4.4 Timing Performance . . . 47
4.5 High-Rate QKD Demonstration Results . . . 49
4.6 Conclusion . . . 51
5 Multi-Photon Detection **53**
5.1 Detection Dynamics of SNSPDs . . . 55
5.2 Experimental Results . . . 57
5.3 Conclusion . . . 64
6 Free-Space Communication **65**
6.1 Atmospheric Effects . . . 66
6.1.1 Scattering and Absorption . . . 67
6.1.2 Turbulence . . . 68
6.2 Multi-Mode Delay Interferometer Design . . . 70

6.2.1 Design Requirements 72
6.3 Performance Simulation 74
6.3.1 Optical Design Modeling and Simulated Performance 76
6.4 Construction 78
6.5 Measurement Results and Discussion 82
6.5.1 Interference Characterization 84
6.5.2 Spatial Mode Performance 88
6.5.3 Thermal Performance 91
6.6 Conclusion and Future Measurements 94
7 Conclusion **96**
7.1 Thesis Summary 97
7.2 Future Directions 98
A Time-Delay Interferometer Derivations **100**
A.1 Constraint Derivations 100
A.1.1 Optical Path Difference 101
A.1.2 Field Widening 102
A.1.3 Thermal Compensation 102
A.2 Optimization Procedure with Air Gap 103
A.3 Optimization Procedure without Air Gap 105
Bibliography **106**
Biography **115**

List of Figures

2.1 Simplified schematic of a 14 bit BB84 protocol using linear polarization states of a single photon. 13

2.2 Discrete time bins comprising a d-dimensional quantum state in a time-phase encoded QKD protocol. 18

2.3 Time-delay interferometer. 19

2.4 Time-phase protocol with $d = 2$. 20

2.5 Time-phase protocol with $d = 4$. 22

2.6 Phase basis measurement on the state $|f_0\rangle$ for $d = 4$. 24

3.1 Cryostat model and assembled system view. 28

3.2 Cooling data for the GM 4 K cooler and 1 K sorption fridge. 29

3.3 Spectrum analyzer traces of noise data before and after filtering. . . . 31

3.4 Simple SNSPD circuit and photon detection waveform. 33

4.1 Detection efficiency of the detector used in our amplifier study, measured at 1550 nm. 37

4.2 Simplified schematic of the SiGe Op-Amp in a non-inverting setup coupled to the SNSPD. 38

4.3 Performance characterization of the SiGe Op-Amp. 39

4.4 Simplified circuit schematic of the detector and GaAs MMIC amplifier setup. 41

4.5 Performance characterization of GaAs MMIC read-out scheme. 42

4.6 Photon detection characterization of GaAs MMIC read-out scheme with an SNSPD. 43

4.7 Maximum count rate measurement using different amplifier read-out schemes 46

4.8 Detector timing resolution using different amplifier read-out schemes. 48

4.9 Experimental setup for the time-bin encoded QKD demonstration. . . 50

4.10 Results of the time-bin encoded QKD demonstration with $d = 4$. . . . 52

5.1 Detection schematic for collecting undifferentiated detection waveforms generated at the SNSPD. 56

5.2 Experimental setup to create short-duration, multi-photon wavepackets. 58

5.3 Photon detection waveforms for $n = 1, 2$, and 3 photons. 59

5.4 Histograms of the peak height of differentiated detection waveforms. . 61

5.5 The effect of dark counts on the distribution of differentiated waveform peak heights. 63

6.1 HiTRAN simulation of a 30 km tropical path including losses from Mie scattering and molecular absorption. 68

6.2 Results of the turbulent simulation analysis. 70

6.3 Simplified schematic of a Michelson-type interferometer. 71

6.4 Angular bandwidth about the central ray of the multi-mode interferometer. 76

6.5 Simulated thermal performance of the multi-mode interferometer. . . 77

6.6 Zemax simulation results of the long arm beam path. 79

6.7 CAD schematic of the interferometer with input and output beam steering and coupling optics. 80

6.8 Schematic of the interferometer experimental setup. 83

6.9 Temperature control of the interferometer bottom plate. 84

6.10 Schematic of the interferometer experimental setup. 85

6.11 Interference fringes for SM and MM (50 μm core fiber) input beams. . 86

6.12 Spatial mode characterization from a 50 μm and 105 μm core fiber. . . 89

6.13 Multi-mode interference characterization as a function of the input spatial mode. 90

6.14 Example measurement of the output power from the interferometer while the system reaches thermal equilibrium. 92

6.15 Multi-mode interference characterization as a function of temperature. 93

List of Abbreviations and Symbols

Symbols

$\|f_m\rangle$	Phase state
$\|t_n\rangle$	Time-bin state
α_i	Coefficient of thermal expansion
β_i	Effective index of refraction
Δ	Optical path-length difference in meters
Δ_t	Optical path-length difference in seconds.
θ_0	Input offset angle
θ	Deviation from input offset angle
μ	Mean photon number
Φ	Sine of the input offset angle
λ	Optical wavelength
n_i	Index of refraction

Abbreviations

ADC	Analog-to-digital converter
AOI	Angle of incidence
BS	Beamsplitter
BER	Bit-error-rate
CAD	Computer animated drawing

CNC	Computer numerical control
CTE	Coefficient of thermal expansion
DC	Direct current
FPGA	Field-programmable gate array
FWHM	Full-width at half-maximum
GaAs	Galium arsenide
GM	Gifford-McMahon
HiTRAN	High resolution atmospheric transmission
IM	Intensity modulator
MMIC	Microwave monolithic integrated circuit
Mcps	Million counts-per-second
MM	Multi-mode
MoSi	Molybdenum silicide
MUB	Mutually unbiased basis
NIR	Near-infrared
NbN	Niobium nitride
NIR	Near-infrared
NIST	National Institute of Standards and Technology
NA	Numerical aperture
Op-Amp	Operational amplifier
OPD	Optical path-length difference
PID	Proportional-integral-derivative
PM	Phase modulator
PMT	Photomultiplier tube
PBS	Polarizing beamsplitter
SKR	Secret key rate

SLM	Spatial light modulator
SM	Single-mode
SNR	Signal-to-noise ratio
SiGe	Silicon germanium
SPAD	Single-photon avalanche diode
SLM	Spatial light modulator
SPAM	State-preparation and measurement
SPDC	Spontaneous parametric down conversion
SNSPD	Superconducting nanowire single-photon detector
TCSPC	Time-correlated, single-photon counter
TEC	Thermo-electric cooler
WDM	Wavelength division multiplexing
WSi	Tungsten silicide
ULE	Ultra-low expansion
QKD	Quantum key distribution

Acknowledgements

It's not a sprint, it's a marathon - a cliched phrase often overused to convey patience or perseverance. But, in my pursuit of a Ph.D. it is quite a fitting one. Like running a marathon, earning a Ph.D. requires extensive planning, discipline, motivation, and often lots of coffee - the gatorade of the graduate student. There are long hours spent doing repetitive tasks, with the occasional soaring triumph, and the always poorly timed injury in the form of a malfunctioning instrument. The footsteps of progress move forward at whatever speed they can manage to eventually cross the tape. As is also the case with running, the individual will cross the finish line alone, but the feat is never accomplished in a vacuum. I have been incredibly fortunate to work with a long list of exceptional people throughout my five years at Duke, and I would like to thank them here.

First, I would like to thank Prof. Dan Gauthier and Prof. Jungsang Kim for allowing me to work on this project. They have been instrumental in all of my achievements and have challenged me to become a better scientist. I would like to thank my advisor, Jungsang, for giving me an opportunity to join his research group and work on this project and always keeping it well funded. I appreciate his willingness to dedicate time and effort to me with several projects also needing attention. I have also had the great privilege of working with Dan for the entirety of my project. Though not listed as my advisor, Dan has been just as instrumental to my development and I am thankful to have been given the time and effort as if I was one of his students.

Without a senior student or post-doc working on this project, I greatly appreciate the support and guidance that Dan and Jungsang have constantly provided.

Thank you to my professors at Centre College; Prof. Jim Kelly, Prof. Jason Neiser, and Prof. Phil Lockett, who opened up the exciting world of physics and started me on this path. Thank you to my committee members: Prof. Hisham Massoud, Prof. Martin Brooke, and Dr. Aaron Miller, for their time and contribution toward my degree. Thank you to Dr. Miller for the helpful discussions about detectors, allowing us to test new devices, and contributing to the discussion of exciting new results. I am thankful for the interactions I had with Dr. Sae Woo Nam and Dr. Varun Verma at NIST, Dr. Matt Saw, Dr. Francesco Marsili and Dr. Emma Wollman at JPL, and Prof. Paul Kwiat and his group at Illinois University. Thank you to Amy Kostrewa, Tony Strimple, Alex Naseree, and Angela Coachman for their logistical help and accepting my late forms. Thank you to Richard Nappi for always being willing to offer help and strike up a conversation. Thank you to Phil Grosshans and Margo Ginsberg for answering countless questions, cleaning up my shopping carts, and being a friendly face every day in the office. I am grateful for the funding support from the Office of Naval Research and the National Aeronautics and Space Administration.

In addition to the people who have mentored me, I have also worked alongside some exceptional people in each project which have resulted in great experiments and great friendships. It was a pleasure to work with Dr. Taimur Islam on the QKD system and I enjoyed the hours spent together setting up the experiment. I learned as much science as I did hard work from him. It was a pleasure to work with Kathryn Nicolich and Dr. Greg Lafyatis on the multi-photon detection experiments. Though I interacted with them mostly through video-conferencing or emails, I enjoyed the process of navigating new results together and coming up with new experiments (sorry you got stuck with the theory..). My role in both of these projects was more enjoyable and more successful because I was able to work with these three exceptional

people.

I am thankful for the support and friendship of the MIST, QElectronics, and Brown labs. Thank you to Dr. Geert Vrijsen (and Dr. Sara Gamble), Dr. Stephen Crain (and Megan), Dr. Emily Mount (and Danny), Dr. Rachel Noek (and Akita), Dr. Volkan Inlek (and Erin), Dr. Meg Shea (and Russ) whom have been helpful in many ways and have also become very close friends. Though our overlap was brief, I enjoyed the beginning of this project building the cryostat with Dan Renaud. Thank you to Tripp Spivey, Yuhi Aikyo, and Chao Fang for the friendship and camaraderie as we navigated classes, research, and basketball games together.

Lastly, I would like to thank my family for their love and support throughout my education. To my parents: I have always been put in a position to succeed throughout my life and in every facet of it. Everything that has followed is all due to the hard work you two have done. You have been the example of positivity, dedication, and kindness that I strive toward. To my brother, Dr. Calvin Cahall: It as been a real luxury to go through college and graduate school alongside my best friend. I am grateful for you always being a willing sounding board when things in the lab are going well or, more often, not working. You're a fantastic scientist and I am constantly impressed by your abilities, even though you beat me. To my wife, Bekah: not only would this have been hard without you, it would not have been possible. You have been my unwavering encouragement in frustrating times, picking up the slack more than your share at home, and have listened to countless rants, exciting results, and boring practice talks. I cannot thank you enough for the sacrifices you have made for me. Thank you.

1

Introduction

The Fifth Solvay Conference convened in 1927 and roughly marked the birth of a new field of physics known as quantum mechanics. The world's leading physicists discussed the inability to predict an observable quantity of a microscopic system's state; whether velocity, spin, or even its physical manifestation as with the photon. This paradigm is in stark contrast to the predictability of a classical system's evolution obeying Newtonian mechanics. Just as the Fifth Solvay Conference marked a new era in physics, Richard Feynman's quantum simulator (Feynman, 1982) began an exciting new subset of quantum physics, known as quantum information.

A quantum simulator was a novel idea, but experimental research in quantum information did not catalyze until work published by Peter Shor in 1994. He extended the applicability of Feynman's vision of quantum simulators to quantum computational devices by developing an efficient prime factorization algorithm on a so-called quantum computer (Shor, 1994). The algorithm, which became known as Shor's algorithm, demonstrated that a theoretical quantum computer could factor a large number in to two primes in polynomial time. The prime-factorization problem is a practically important problem because it is believed to be computationally difficult

to solve using classical computers. The implication of Shor's algorithm is that a quantum computer has the potential to provide an exponential speed-up over the best known algorithms using classical computers. This breakthrough encouraged a large research effort to develop scalable and robust quantum computation hardware that continues today (Monroe and Kim, 2013; Barends et al., 2014).

1.1 Secure Communication

Shor's algorithm has a significant impact on encrypted classical communication such as internet traffic and wireless communication. Modern communication systems are secured against eavesdroppers using an encryption technique known as public key encryption. Protocols of this type were deployed on a large scale after work by Rivest, Shamir, and Adleman (RSA) and are now ubiquitous in the modern age of global communication and internet commerce (Rivest et al., 1978). However, public key protocols such as RSA are secure to eavesdropping attacks only under the assumption that an attacker cannot quickly factor a large number into two primes. Shor's algorithm implies that communication secured using RSA encryption is vulnerable to an attacker with a quantum computer.

In the years following Feynman's quantum simulator researchers proposed hypothetical experiments using the resources of quantum systems such as quantum money that is impossible to counterfeit (Wiesner, 1983). However, it was Shor's algorithm that revived the decade-old work by Charles Bennett and Gilles Brassard on quantum-enabled secure communication (Bennett and Brassard, 1984). Their protocol, which came to be known as BB84, allowed two distant parties to securely share a message via a protocol called quantum key distribution (QKD). Later Artur Ekert framed the protocol in an equivalent scheme using non-local quantum correlations called entanglement (Ekert, 1991). Though distant, the prospect of a world filled with functioning quantum computers magnified the vulnerability of public key pro-

tocols and motivated experimental research efforts in quantum cryptography (here the phrases quantum cryptography and quantum key distribution are used interchangeably, though quantum key distribution is a subset of the larger field of quantum cryptography). The first QKD protocol was demonstrated in 1989 using linear polarization states and the BB84 protocol (Bennett and Brassard, 1989) and since then QKD has been a highly active area of research including commercially available products (IDQuantique, 2019).

In this chapter I discuss the details of public and private key encryption techniques to motivate the utility of QKD. Then, I detail the limitations of current QKD systems and the experimental requirements to realize a robust and high-rate system for free-space applications.

1.1.1 Public Key Cryptography

Cryptography is a process that enables two parties to communicate securely in the presence of an eavesdropper. In typical cryptographic protocols a plain text message is encoded by the sender (Alice) with an encryption key. The key used for encryption is a random bit string that interacts with the message to create text that will reveal no meaningful information if intercepted. The encrypted message is sent to the receiver (Bob) where it is decrypted using a different key. This type of protocol is known as asymmetric encoding. Modern, classical communication such as internet traffic or other sensitive communication is secured using a public key protocol. In public key protocols, such as RSA, the encryption key is transmitted from Bob to Alice through a public channel where she uses it to encrypt her message. Once the message is received by Bob he decrypts the message with his decryption key that is kept private. Since the encryption key is made public it is important for the decryption key to remain private or the message is susceptible to attacks.

In public key protocols the decryption key is produced from the encryption key by

a process that requires factoring a large number into two primes. The security of the protocol hinges on the fact that it is computationally difficult to do the factorization, known as the prime factorization problem. The best known factorization algorithms performed on classical computers require exponentially scaling resources and are therefore very inefficient.

1.1.2 Private Key Cryptography

Unlike public key protocols, private key cryptography is a simple alternative that does not rely on assumptions about an eavesdropper's computational power to guarantee security. In a private key cryptosystem Alice and Bob share the same random bit string (symmetric encoding) to encrypt and decrypt the message. To gain information about the message an eavesdropper would need to correctly guess the key to perform the decryption. The probability to correctly guess the random bit string goes as $1/2^N$ where N is the number of bits contained in the message. For example, the probability to guess a small key of 128 bits is $\sim 10^{-40}$. For the encryption to remain secure, each set of cryptographic keys must be used only once and the length of the key must be as long as the message they wish to share. Therefore, Alice and Bob must produce a new key for each message.

Despite the simplicity of the protocol, the distribution of keys between the two parties over an unsecured communication channel is non-trivial. However, if Alice and Bob communicate through a quantum channel then they can securely share a key using a quantum key distribution (QKD) protocol. QKD enables the sharing of classical bit strings using quantum states for transmitting the information and probing the security of the quantum channel. Once the keys have been distributed then Alice and Bob can communicate classically using a private key protocol. The ambiguity of a quantum state is used as a resource to limit the information that an eavesdropper can obtain. Additionally, if some information about the key is

obtained then this can be detected. Ideal QKD makes no limiting assumptions about an eavesdropper's computational power, including allowing access to a functional quantum computer, and guarantees unconditional security.

1.2 Quantum Communication Systems

Several experimental challenges currently limit a large-scale deployment of a national or global QKD system. The most significant limitation to current systems is that they lack a secret key rate (SKR) fast enough to be practically useful for modern communication. The current state-of-the-art SKR for QKD systems is < 100 million bits-per-second (bps) (Islam et al., 2017a), compared to classical communication that can operate in the range of $1 - 10$ Gbps (Google, 2019). A unique private key must be generated for each secure message and therefore the SKR will limit the data transfer rate by a factor ~ 100. The largest contribution to the rate limitation is due to large detector dead-times in single-photon counting detectors. Typically, the detector dead-time is > 10 ns and therefore limits the detection rate to < 100 million counts-per-second (cps).

Further limitations are imposed by the infrastructure used in classical telecommunications. Encoding schemes such as orbital angular momentum, spatial mode, or polarization are not compatible with the classical infrastructure which typically use single-mode fibers for long distance communication. Other components, such as optical amplifiers, are often placed in the channel that amplify classical optical signals to increase the link distance. Classical amplifiers such as these are not useful for quantum communication because the no-cloning theorem (discussed more in Chapter 2) prohibits an unknown quantum state from being copied or amplified. These infrastructure limitations make it difficult to deploy a quantum network over the existing infrastructure, and therefore could make installing new infrastructure necessary to establish quantum communication links.

However, specific applications such as free-space optical communication links between naval ships, or ground-to-satellite communication, are great niche applications for quantum communication schemes. Additionally, free-space communication is advantageous because the channel loss scales as the second power of the channel length L ($\sim L^2$) whereas the loss in optical fiber scales exponentially ($\sim e^{\alpha L}$). Historically, free-space communication is performed using radio-frequency (RF) signals which lack significant directionality and require public-key encryption since the message can conceivable be collected by any receiver within range of the transmission. The development of free-space quantum communication links are practically important because they can likely be the basis for large scale quantum networks or a quantum internet where satellites can act as nodes connected by free-space communication links.

1.3 Thesis and Contribution Overview

In this thesis I discuss the work that I have completed to advance the capabilities of quantum communication systems, specifically towards high-rate and free-space implementations. I begin with an introduction to the quantum information framework that provides the foundation of basic quantum computation and quantum communication principles in Chapter 2. Quantum key distribution protocols are also discussed in detail, beginning with a general description of the BB84 protocol, then with a specific treatment of the time-phase protocol that is the basis of our experimental demonstration.

The time-phase protocol that is discussed in Chapter 2 was conceived by Prof. Daniel Gauthier and the security proof for the protocol was completed by Dr. Charles Lim and Dr. Nurul T. Islam. Dr. Islam constructed and characterized the transmitter and recorded the published QKD data (Islam et al., 2017a). I assisted in the integration of the receiver and transmitter, optimizing the receiver for QKD measurements, and

performed preliminary measurements with Dr. Islam. The quantum communications system requires specific infrastructure for an experimental realization. I describe the receiver infrastructure in detail in Chapter 3. The infrastructure includes a cryostat system needed for the operation of superconducting nanowire single-photon detectors (SNSPDs). I also describe the operating principles of the detectors. I constructed the cryostat with another graduate student, Daniel Renaud, and then I performed the detector testing and characterization.

In Chapter 4 I describe the optimization of the receiver detailed in Chapter 3 to achieve high timing resolution and high maximum count rates, performance characteristics that are necessary for realizing a high-rate communications system. The main results from Chapter 4 are novel cryogenic amplifiers that enhance single-photon detector performance and are scalable to multiple detector channels. I demonstrate timing resolution of 35 ps, a maximum count rate of > 20 million counts-per-second, while maintaining < 3 mW power consumption measured at an operating temperature of 4 K. I constructed and tested the amplifier circuits, analyzed the data in collaboration with Prof. Gauthier, and recorded the published data (Cahall et al., 2018).

Chapter 5 contains a novel contribution to quantum communication and to the field of quantum optics in general. In this chapter I discuss the first demonstration of multi-photon detection in a conventional SNSPDs. Multi-photon resolution is the result of subtle changes in the dynamics of the photon detection event and are verified experimentally. I demonstrate the detection of up to four photons with a high fidelity discrimination of greater than 99.9% accuracy between single-photon and multi-photon events. This work is supported by a collaboration with Prof. Gauthier's group at The Ohio State University (OSU) including Dr. Gregory Lafyatis and Kathryn Nicolich. A theoretical model supporting our experimental findings was developed by the OSU team and I designed the experiment using the transmitter

developed for the QKD protocol. I recorded the published data (Cahall et al., 2017) and performed the data analysis with support from the OSU team.

A free-space communication demonstration requires the receiver to support multiple spatial modes that are not present in a single-mode system such as long-distance fiber-based networks. In Chapter 6 I describe the design of a multi-mode receiver where the largest contribution of my effort was in the design and construction of a multi-mode time-delay interferometer. The interferometer is required for executing the phase-basis measurement in time-phase QKD. I designed and constructed an interferometer with a 5 GHz free-spectral range achieving $> 98\,\%$ interference visibility with negligible dependence on the mode structure of the input beam and modest temperature fluctuations. Additionally, the interferometer demonstrated a small path-length shift of $130\,\mathrm{nm}/^{\circ}\mathrm{C}$, allowing for great thermal stability with modest temperature control. I conceived the design and performed the simulations, construction, characterization, and data collection. Design and construction feedback was provided by Prof. Gauthier.

I conclude the thesis with a discussion of future of quantum communication protocols and the outlook for free-space protocols. I discuss additional experiments and improvements that can be done to enhance the multi-photon capabilities of SNSPDs. Additionally, I discuss the improvements that can be made to the interferometer design as well as more complicated prototypes that can be constructed.

2

Quantum Communication

This chapter begins with the necessary background to understand the basic principles of quantum communication. I introduce the fundamentals of quantum information and detail the first quantum key distribution protocol: two-dimensional BB84. Finally, I detail the time-phase protocol that is the protocol that we demonstrate experimentally.

2.1 Quantum Foundations

The building blocks of classical computation are digital logic levels, known as bits, where information is encoded in discrete states labeled '0' and '1.' Typically, the physical representation of a bit is the voltage on a wire or at a junction that is either 'high' or 'low' relative to some threshold. Quantum information uses eignestates of a quantum system to store quantum bits, often referred to as qubits. Similar to classical bits, qubit states are labeled $|0\rangle$ and $|1\rangle$, where it is common to use Dirac notation to denote quantum states (Nielsen and Chuang, 2010). Physically, the states $|0\rangle$ and $|1\rangle$ can be any set of orthogonal basis states, such as the polarization states of a single photon or the spin states of a trapped atomic ion (Cirac and Zoller, 1995;

Monroe and Kim, 2013).

The laws of quantum physics allow the qubit to exist in a continuous, linear combination of the basis states with associated complex probability amplitudes. This property is known as the superposition principle. The probability amplitudes are complex because the quantum states behave like waves and therefore have an associated magnitude and phase, both of which can be surmised in a complex number. In general the state of a qubit $|\psi\rangle$ is written as,

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,, \tag{2.1}$$

where the complex probability amplitudes are given by α and β. The probability amplitudes must obey the normalization condition $|\alpha|^2 + |\beta|^2 = 1$. The superposition principle is a computational resource that allows quantum computers to test many inputs simultaneously, whereas classical computers must test each input individually. This idea of parallelism is exploited in Shor's algorithm and Grover's search algorithm (Grover, 1996) . Additionally, superposition implies a necessary ambiguity in a qubit's state. This ambiguity is exploited in the quantum communication protocols that will now be discussed in detail.

2.2 Quantum Key Distribution

Two principles of quantum physics enable the secure communication achieved by QKD. These principles are the information/disturbance trade-off and the no-cloning theorem (Nielsen and Chuang, 2010). The information/disturbance trade-off states that any information gained about the state of a quantum system must necessarily disturb the state. The strongest case of this disturbance is a projective measurement where the state is projected onto some basis. For example, consider a projective measurement of the state $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ into a basis consisting of the states

$\{|0\rangle, |1\rangle\}$, referred to as the computational basis. A measurement outcome of $|0\rangle$ will leave $|\psi\rangle$ in the (re-normalized) state $|\psi\rangle = |0\rangle$ immediately following the measurement. The information/disturbance trade-off implies that information that is gained about a quantum state can be quantified. One might suggest that this can be circumvented by copying the quantum state and performing a measurement on the copied state (or many copies of the state). However, copying an arbitrary quantum state is prohibited by the no-cloning theorem.

Consider Alice and Bob wish to communicate a secure message. They can use quantum key distribution to exchange a cryptographic key to be used in a private key protocol, discussed in the previous chapter. To complete a QKD protocol they communicate through a quantum channel using single-photon states. Additionally, they have access to a classical communication channel. Both channels are assumed to be accessible by an eavesdropper, Eve. Photonic states have many degrees of freedom useful for encoding information including polarization, orbital angular momentum (Leach et al., 2012), and time-bin (Brougham et al., 2016), the latter being an example of a basis that can support high-dimensional encoding. Let d be the dimension of the Hilbert-space used for the encoding where $d = 2$ are referred to as qubit protocols and $d > 2$ are high-dimensional states call qudits. The traditional BB84 protocol described below is a qubit protocol that uses linear polarization states of a photon.

2.2.1 BB84

Classical bit values '0' and '1' are encoded in one of two bases that span a two-dimensional Hilbert space. The first encoding basis (computational basis) is comprised of horizontal and vertical polarization states where the states $|0\rangle$ and $|1\rangle$ are given by Eq. 2.2. The second encoding basis is a diagonal basis and is defined as equal superpositions of the the $|H\rangle$ and $|V\rangle$ states, shown in Eq. 2.2.

$$\begin{array}{ll} \text{Computational Basis} & \text{Diagonal Basis} \\ |0\rangle = |H\rangle & |0\rangle = |+45\rangle = (|H\rangle + |V\rangle)/\sqrt{2} \\ |1\rangle = |V\rangle & |1\rangle = |-45\rangle = (|H\rangle - |V\rangle)/\sqrt{2} \end{array} \tag{2.2}$$

The diagonal basis has a non-zero overlap with the computational basis. Two such bases are said to be mutually unbiased (MUB) because a projection of any state in to the opposite basis is uniformly distributed. The significance of uniformly distributed measurement results is that a projection of a state into the opposite basis will yield a random outcome. For the qubit protocol shown here, $|| \langle H| \pm 45\rangle ||^2 = || \langle V| \pm 45\rangle ||^2 = 1/2$.

A simplified BB84 protocol is shown in Fig. 2.1. The protocol begins with Alice choosing an encoding basis (computational or diagonal) and a bit value to encode (0 or 1) at random. Alice sends the encoded photons to Bob where he measures his photons in a basis chosen at random. His measurement basis is chosen at random because he has no prior knowledge of Alice's basis choice. Measurement results of $|0\rangle$ and $|+45\rangle$ denote a classical bit 0, and $|1\rangle$ and $|-45\rangle$ denote a classical bit 1. Once all photons have been transmitted Alice and Bob publish each of their basis choices over the classical channel. The times where Alice and Bob have chosen different bases will yield random results and so they discard all instances where they chose different bases. After this step Alice and Bob share a raw key.

The raw key will contain errors due to losses in the channel or Eve's disturbance (more on Eve's attacking strategies below). The source of the error is not known and so all errors may conservatively be assumed to be the result of information gained by Eve. Alice and Bob will estimate the error rate in the raw key by publishing half of their bits and do a bit-wise comparison. The error rate in this subset is assumed to be representative of the full set. If the bit-error-rate (BER) is above a certain

Bit Value	1	0	0	0	1	0	1	1	0	0	1	0	1	1
Alice's Basis Choice	+	+	x	+	x	x	x	+	+	x	x	+	x	+
Encoded State	↑	→	↗	→	↖	↗	↖	↑	→	↗	↖	→	↖	↑
Bob's Basis Choice	+	x	x	+	+	+	x	x	+	+	+	+	x	x
Bob's Result	↑		↗	↑			↖		→			→	↗	
Raw Key	1		0	1			1		0			0	0	
Subset – Final Key	1						1		0					

FIGURE 2.1: Simplified schematic of a 14 bit BB84 protocol using linear polarization states of a single photon.

threshold then the protocol is aborted. The value of this threshold depends on the specific protocol being used. For BB84, the BER threshold is 11% (Shor and Preskill, 2000). If the BER is lower than the abort threshold, then a process called privacy amplification is used to make the number of errors arbitrarily small (Impagliazzo et al., 1989). This process involves randomly sampling a subset of the key by communicating only the bit positions they wish to keep. Random sampling reduces the errors and also Eve's knowledge of the key. After privacy amplification the protocol is complete and Alice and Bob share a secure key.

2.3 Security of QKD

A detailed survey of all possible attack strategies and security proofs are outside the scope of this thesis, and so I will give a brief overview of attack strategies that Eve can

use to gain information about the transmission (Scarani et al., 2009). Each attack strategy has an associated level of security that the protocol is protects against.

2.3.1 Individual Attacks

Individual attacks are the simplest strategy that Eve can use. This class of attacks involve Eve interacting with each state of her choosing on an individual basis (*i.e.* her interaction is not informed by any result from a previous interaction). Intercept-and-resend is an example of an individual attack where Eve intercepts the state and performs a measurement. The measurement collapses the state and Eve sends the resulting state to Bob. Eve has no prior knowledge of Alice's encoding basis and so Eve can only choose her measurement basis at random.

To see how this attack strategy can be detected consider the BB84 protocol above where Eve uses the intercept-and-resend strategy. For simplicity, we will only consider the cases where Alice and Bob have chosen the same basis for encoding and measurement, and that Eve intercepts every state. As stated above, Eve must randomly choose a basis in which to perform her measurement. Half of her choices will be correct and in these cases her measurement will not change the state of the photon. Therefore, she will obtain the bit value undetected. However, half of the time she will choose the wrong basis and as a result will project the photon in to the opposite basis to Alice and Bob's choice. For these cases Bob's measurement will be random and therefore produce the wrong bit value for half of these instances, resulting in an overall error rate of 25%. An error rate of this magnitude will result in aborting the communication. If Eve chooses to intercept only a fraction of the states then the error rate will be lower but so too will the number of bits she obtains. Her information can be made arbitrarily small after the privacy amplification step.

2.3.2 Collective Attacks

This class of attacks is similar to individual attacks in that Eve interacts with each state individually, but in a collective attack Eve can store the information she receives in a perfect quantum memory. A quantum memory allows Eve to preserve the quantum state she has intercepted until after Alice and Bob publish their basis choice. Knowledge of the basis choice enables Eve perform the proper measurement and gain complete knowledge about the intercepted state.

2.3.3 Coherent Attacks

Coherent attacks are the strongest class of attacks because they are the most lenient in the restrictions placed on Eve. For this class of attacks Eve's actions are only limited by the laws of Physics. This implies that Eve has unlimited resources including a quantum computer and a perfect quantum memory. Additionally, Eve's strategy can be much more complex than an individual attack. For example, Eve can change how she interacts with one photon conditioned on the outcome of a previous interaction or measurement. Coherent attacks are the most difficult to prove security against because of the near infinite strategies that Eve can use.

2.3.4 Side-Channel Attacks

An additional class of attacking strategies called side-channel attacks exploit experimental non-idealities that are specific to the QKD protocol. One such example is a photon-number-splitting (PNS) attack (sometimes also classified as a stronger individual attack). Ideally, the source in a QKD system would use an on-demand single-photon source. However, these types of sources are very complex or lack the speed and efficiency needed to execute a high-rate QKD demonstration despite great progress (Eisaman et al., 2011). It is much more pragmatic to use a coherent source such as a laser where weak coherent states replace pure single photon states. Weak

coherent states are created by attenuating the intensity of the laser to a mean photon number $\mu \leqslant 1$. A small value for μ will produce single-photon states but because coherent sources are Poissonian there is a non-zero probability multi-photon states will be created. The probability for an n-photon number state to be produced from a coherent source with a mean photon number μ is given by the Poisson distribution,

$$P(n) = \frac{\mu^n e^{-\mu}}{n!}. \tag{2.3}$$

For example, a mean photon number $\mu = 1$ gives the following probabilities: $P(n = 1) \approx 0.37$, $P(n > 1) \approx 0.26$.

Multi-photon states are susceptible to the PNS attack because Alice's encoding is performed on each photon contained in the wavepacket. Therefore, Eve has an opportunity to collect one photon containing the same information that Bob receives. Eve can store her collected photon in a quantum memory and measure it after the bases have been published without disturbing the outcome of Bob's measurement.

2.4 Time-Phase QKD

Experimental realizations of QKD systems are often hindered by non-idealities in the equipment used to generate and measure the photons. Rate limitations are dominated by detector saturation and dead-time, and so it is advantageous to increase the channel capacity by encoding bits in a high dimensional Hilbert space. We use a time-phase encoding (Brougham et al., 2016; Islam, 2017) because it can support a high dimensional ($d > 2$) encoding. Qudit protocols can transmit up to $\log_2 d$ bits per photon, whereas qubit protocols such as BB84 are limited to a single bit per photon. Additionally, high-dimensional schemes can tolerate a higher BER which enable longer communication distances (Scarani et al., 2009).

Our time-phase protocol consist of two mutually unbiased bases that are referred

to as the temporal or time-basis, and the frequency or phase-basis. Information is encoded in the temporal basis and the phase basis is used to check for the presence of Eve (Brougham et al., 2013). This is in contrast to the BB84 protocol discussed above where each basis (computational and diagonal) perform both tasks of data transmission and security. Temporal states are constructed by placing a photonic wavepacket of width δ in a discrete time bin of width τ. We require $\delta << \tau$ such that the wavepacket is well localized in the time-bin. A schematic of the time state $|t_n\rangle$ is shown in Fig. 2.2a. A wavepacket in the n'th time-bin is labeled $|t_n\rangle$, where $n = \{0, 1, ..., d-1\}$ and d defines the dimension of the protocol.

Phase states are constructed with an equally weighted superposition of time states where each time bin carries a specific phase relative to the first bin. The m'th phase state is shown in Fig. 2.2b and is written as,

$$|f_m\rangle = \frac{1}{\sqrt{d}} \sum_{n=0}^{d-1} \exp\left(\frac{2\pi nm}{d}\, i\right) |t_n\rangle\,, \tag{2.4}$$

where the phases are given by the discrete Fourier transform. The phase state $|f_m\rangle$ is shown in Fig. 2.2b.

2.4.1 $d = 2$ Time-Phase

Generation and measurement of the time and phase states is introduced here using a $d = 2$ encoding for simplicity. In our experiment the states are constructed by intensity modulating a continuous-wave (CW) laser source to create short duration wavepackets. The states are highly attenuated to produce weak coherent states with a mean photon number per pulse of $\mu \approx 1$. Phase states are constructed using intensity modulators to create the superposition of time states and an additional phase modulator that modulates the phases of each time bin. The attenuation of the phase states is adjusted such that the probability amplitudes of the entire frame

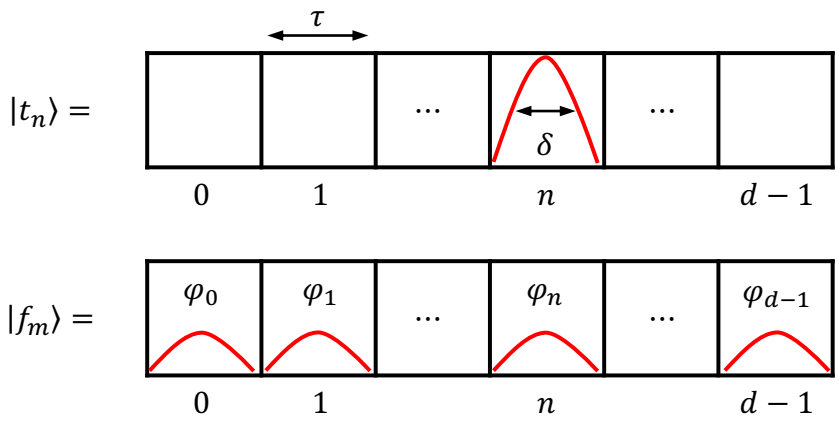

FIGURE 2.2: Discrete time bins comprising a d-dimensional quantum state in a time-phase encoded QKD protocol. (a) A single photonic wavepacket placed in time-bin n defining the state $|t_n\rangle$. (b) A uniform superposition of time-bin states, each with a relative phase ϕ_i, defining the frequency state $|f_m\rangle$.

sum to unity. It is important to use a modulation scheme with a high extinction ratio in order to prevent errors caused by detection events resulting from background photons leaking through modulator. The states for a $d = 2$ time-phase protocol are shown in Fig. 2.4.

A measurement in the temporal basis is performed with a single-photon detector where the electrical signal generated from a detection event is recorded with a high resolution time-tagger. The single-photon detector and processing electronics including amplifiers and time-tagging electronics must have low timing uncertainty (detection jitter) in order to localize the time-of-arrival of the photon with high accuracy. The arrival time of the single-photon detection event is compared to the shared global clock to declare the result of the measurement.

Phase-state measurements require a time-delay interferometer, shown schematically in Fig. 2.3. A phase state entering the interferometer is split by a 50/50 beam-

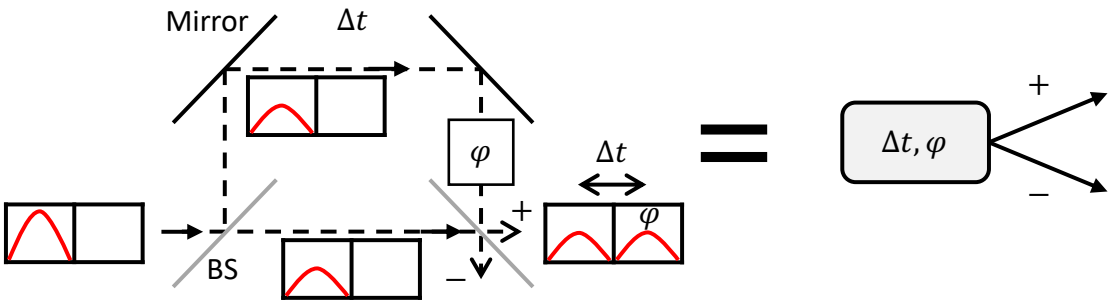

FIGURE 2.3: Time-delay interferometer. The interferometer is characterized by the time-delay (or path-length different) Δt and the phase setting of the long path ϕ.

splitter with half of the wavefunction traveling through a long path and half through a short path. The difference in path lengths is chosen such that the time-delay is equal to τ, or one time bin width. Therefore, the wavefunctions that recombine at the second beamsplitter are shifted by one time bin relative to each other. An additional phase adjustable ϕ is available to tune the phase of the interference fringe, where $\phi = 0$ in the $d = 2$ scheme. Phase tuning is achieved by adjusting the path-length difference on the order of the optical wavelength λ. Additionally, $\lambda/c \ll \Delta t$ and therefore does not effect the time delay.

A phase state that passes through the interferometer tree will result constructive or destructive interference in the shaded time-bin shown in Fig. 2.4b. There is a one-to-one mapping between the phase-state input and the detector in which constructive interference is observed. Therefore, constructive interference is detected at a unique detector, with destructive interference at all other detectors. In the $d = 2$ protocol a photon detection event in the shaded time bin of detector $D0$ ($D1$) indicates a measurement outcome of $|f_0\rangle$ ($|f_1\rangle$). The lobes in the interference pattern lying

outside the shaded time bin are considered losses and do no contribute to the outcome of the measurement. The phase-basis measurement succeeds at a rate of $1/d$, or 50% for the $d = 2$ scheme.

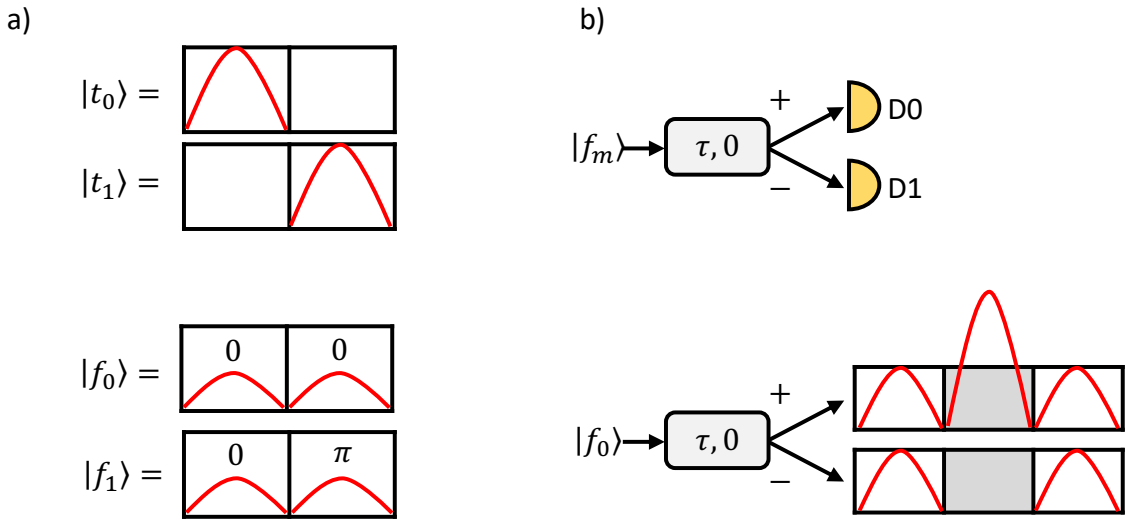

FIGURE 2.4: Time-phase protocol with $d = 2$. (a) Temporal and phase basis states. (b) Time-delay interferometer setup for a $d = 2$ phase basis measurement. Also shown are the interference patters for a measurement on the $|f_0\rangle$ state.

It is straightforward to see that the time and phase bases are indeed a mutually unbiased set. A phase state is constructed from a uniform superposition of time-states and therefore a time-basis measurement will localize the photon to one of the time-bins with equal probability, yielding a random measurement outcome. Similarly, a temporal-state with a photon localized to the first time-bin has equal probability of being detected in the first or second time-bin after passing through the time-delay interferometer, therefore resulting in a random measurement outcome.

To monitor the presence of Eve we look at the statistics of the interference in the phase basis measurement. For the purpose of this example, we assume that Eve uses the simple intercept-and-resend strategy. Only the phase states are used to probe the channel, and so we will focus on the effects that Eve has on the outcome

of the phase basis measurement. The security of channel is assessed at the end of all communication by calculating the visibility of the constructive and destructive interference in the shaded time bin in Fig. 2.4.

Consider Alice sends the f_0 state. The visibility of the interference is defined by

$$\mathcal{V} = \frac{\mathcal{P}_+ - \mathcal{P}_-}{\mathcal{P}_+ + \mathcal{P}_-} \tag{2.5}$$

where $\mathcal{P}_+$ ($\mathcal{P}_-$) is the probability of detecting a photon in the shaded time bin at detector $D0$ ($D1$). A reduction in the counts at detector $D0$ or an increase in the counts at detector $D1$ will degrade the visibility. Consider Eve intercepts the $|f_0\rangle$ state and performs a time-basis measurement where she will localize the photon in the first or second time bin. The temporal basis measurement destroys the coherence between the two time bins and therefore the photon will travel through the interferometer without interfering. For example, a single photon localized in the first time bin has a probability of 0.75 of being detected in the wrong detector ($D1$) or in the wrong time bin of detector $D0$, and therefore will decrease the visibility of Bob's phase basis measurement.

2.4.2 $d = 4$ Time-Phase

As mentioned above, high dimensional schemes can encode multiple bits per photon. Increasing the dimension of the time-phase scheme only requires adding more time bins in the frame defining the state. Increasing the size of the frame also comes at the cost of reducing the number of frames sent per second, potentially decreasing the overall bit rate. However, with current state-of-the-art equipment the state generation rate can be $> 10\,\text{GHz}$ and the maximum count rate of single-photon detectors is typically limited to < 100 million counts-per-second (Mcps), greater than a factor of 10^2 slower. When the state generation rate of the transmitter is

operating far above the detector saturation rate there is no penalty to increasing the dimension of the time-phase protocol because the detection rate will be the limiting factor (until the frame rate is reduced to below the maximum detection rate). Therefore, the bit-rate is doubled when performing a $d = 4$ protocol compared to a $d = 2$ protocol.

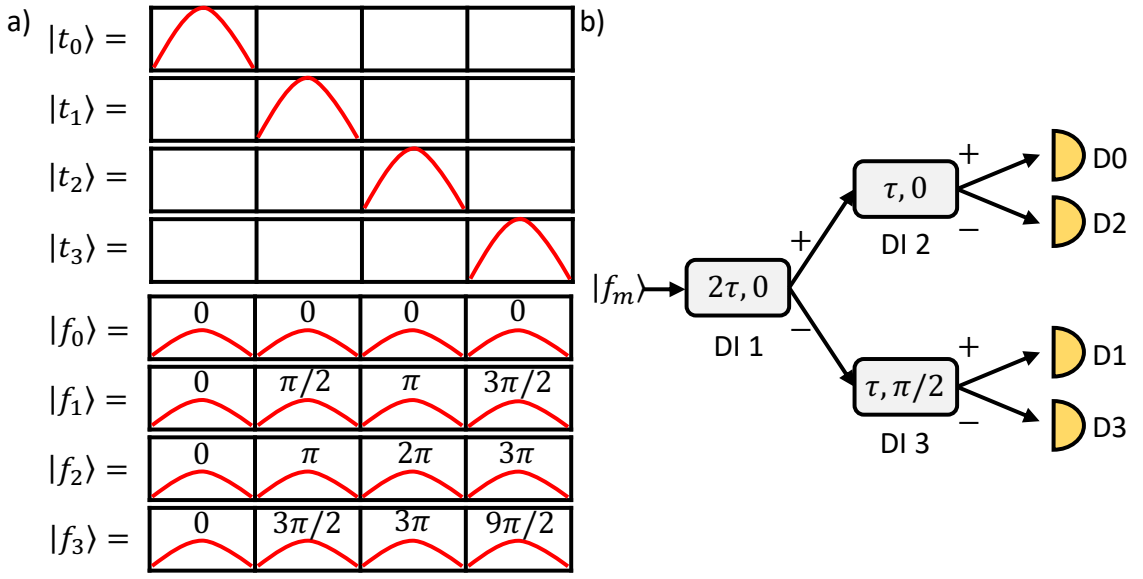

FIGURE 2.5: Time-phase protocol with $d = 4$. (a) Temporal and phase basis states. (b) Cascaded interferometer tree for a $d = 4$ phase basis measurement.

The basis states for a $d = 4$ protocol, shown in Fig. 2.5, are constructed in the same way as those in the $d = 2$ scheme. Temporal basis measurements are also carried out in the same way as for $d = 2$. Phase-state measurements for $d = 4$ require more resources because interference must take place between more than neighboring time-bins. The scheme proposed to measure high-dimensional phase-states uses a cascaded tree of time-delay interferometers (Brougham et al., 2013). A d-dimensional protocol requires $d - 1$ interferometers (with varying timing delays Δt and phase settings ϕ) and d single photon detectors. The interferometric tree for $d = 4$, shown in Fig. 2.5, requires a total of three interferometers where the first interferometer has a time

delay $\Delta t = 2\tau$ and phase offset $\phi = 0$. The second layer has two interferometers, one for each output of the first interferometer, each having a time delay $\Delta t = \tau$ and with phase offsets $\phi = 0$ and $\phi = \pi/2$. Similar to $d = 2$, the output of the interferometer tree for a particular phase state input is a pattern of interference fringes where there is constructive interference in the shaded time bin at one detector and destructive interference at all other detectors. Therefore, there is a one-to-one mapping from the set of phase states inputs to the detectors. The interference fringes for a measurement of the state $|f_0\rangle$ is shown schematically in Fig. 2.6b.

Recent experiments indicate that the communication can be secured using as little as one state from the MUB, therefore reducing the number of interferometers and detectors required (Islam et al., 2018). Additionally, the interferometer tree can be replaced entirely by a measurement scheme where Bob uses a local oscillator to generate a state to interfere with Alice's state (Islam et al., 2019). In this scheme Bob needs only a beamsplitter and two detectors to perform the measurement. These two improvements to the time-phase protocol will not be discussed in this thesis.

2.5 Conclusion

In this chapter I describe the fundamentals of quantum information and the building blocks of QKD. The protocol is enabled by two principles that are fundamental to quantum physics: namely, the information/disturbance trade-off, and the no-cloning theorem. The BB84 protocol is described in detail to introduce the important concepts to design a QKD system. I discuss the time-phase encoded protocol that is the basis for my experimental efforts discussed in the remaining chapters of this thesis. A time-phase encoding is a high-dimensional protocol that is well suited for communication at long distances and in presence of detector saturation.

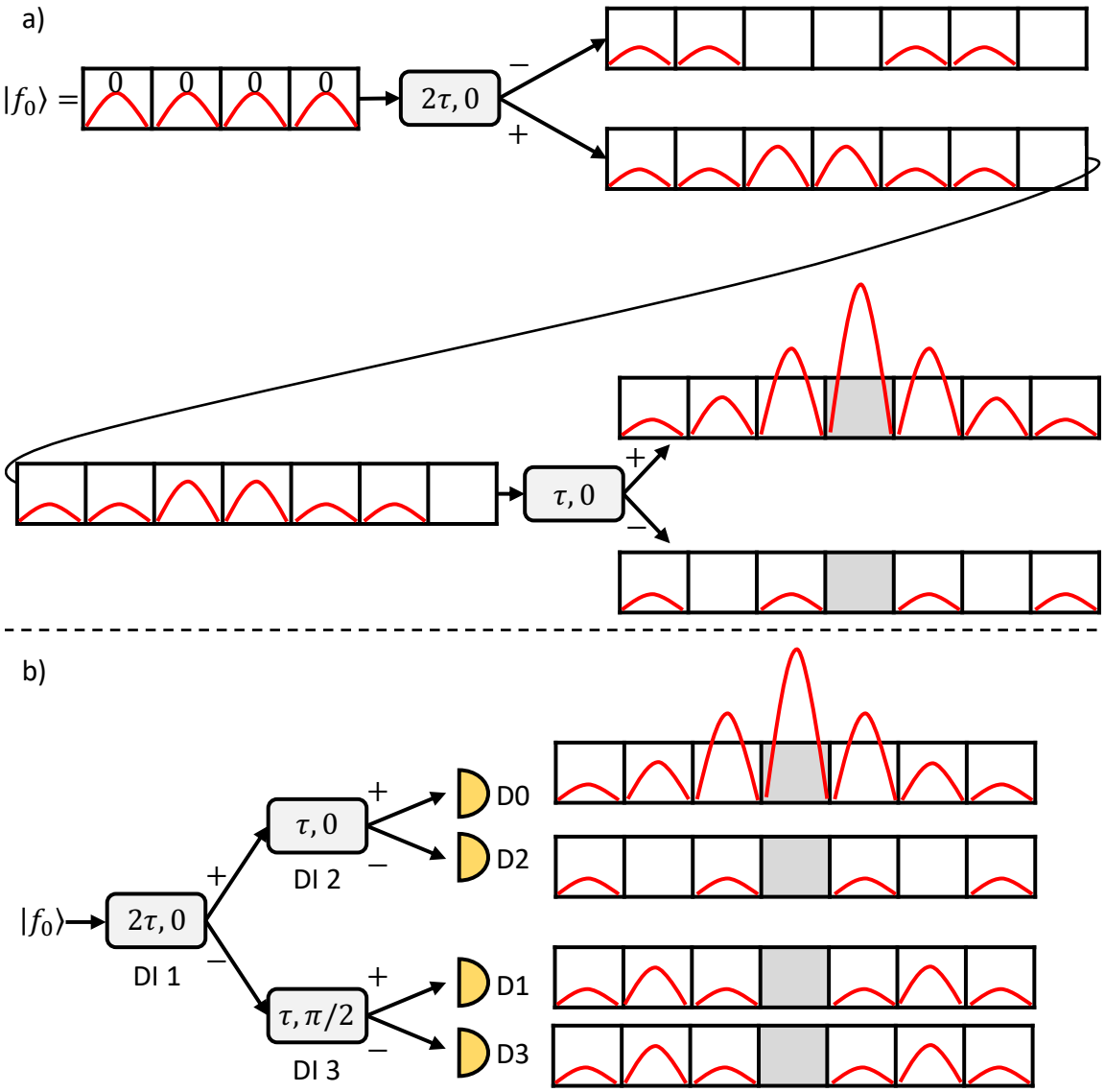

FIGURE 2.6: Phase basis measurement on the state $|f_0\rangle$ for $d = 4$. (a) Interference pattern at each step of the interferometer tree. The schematic only shows the top path after the first interferometer. (b) Fringe patter detected at each detector. The shaded bin indicates the outcome of the measurement.

3

Receiver Infrastructure

A high performing single photon detection receiver is necessary to realize time-bin encoded or pulse-position-modulated quantum communication schemes. Central to the receiver system is the photon detector and the infrastructure that is needed for operation, discussed in this chapter. The performance of the receiver is also highly dependent on the readout electronics used to amplify and measure detection signals, discussed further in Chapter 4. Detector performance is characterized by metrics such as detection efficiency, timing resolution, maximum count rate, and dark count rate. No single detector owns the best performance in all metrics and so compromises must be made that cater to the specific needs of the communication system. In a time-bin encoded protocol a premium is placed on four metrics: detection efficiency, timing resolution, maximum count rate, and dark count rate. In the time-bin encoded protocol discussed in Chapter 2, high detection efficiency and a high maximum count rate will enable the best possible key rate. Dark counts will limit the maximum visibility in the interference measured in the frequency-basis. Poor timing resolution will cause photon detection events to be mistakenly assigned to adjacent time bins, resulting in errors.

Photo-Multiplier tubes (PMT) are a popular commercial single photon detector option but lack high efficiency, especially at longer wavelengths (wavelength considerations discussed more in Chapter 6). Silicon and indium-gallium-arsenide single-photon avalanche diodes (SPAD) have improved efficiency, but suffer in timing resolution and dark count rate (Migdall et al., 2013). Superconducting nanowire single photon detectors (SNSPD) are a relatively new technology compared to the semi-conductor detectors and have demonstrated near unity detection efficiency with sub-Hz intrinsic dark count rate (Marsili et al., 2013), maximum count rates in the range $10 - 100\,\mathrm{Mcps}$ (Kerman et al., 2006), and timing resolution $< 100\,\mathrm{ps}$ (Dauler et al., 2014). SNSPDs have emerged as a leading technology for quantum information science and classical photon-starved experiments and played a crucial role in the recent loophole-free Bell inequality measurements (Shalm et al., 2015) and the Lunar Laser Communication Demonstration (Boroson et al., 2014). Additionally, SNPSDs are featured in quantum communication protocols such as superdense quantum teleportation (Graham et al., 2015) and quantum key distribution (Islam et al., 2017a). The high performance characteristics of SNSPDs make these the detectors the best choice to use for the QKD receiver. Unlike PMTs or SPADs that can operate at room temperature or with modest refrigeration, the operation of SNSPDs require a cryogenic system.

3.1 Cryostat

The nanowire material that comprises the active element in the detector must be cooled to below the superconducting threshold temperature T_C, where T_C is a function of the nanowire material and geometry. The value of T_C determines the refrigeration system required for operation. Typically, SNSPDs require a cryogenic system operating at temperatures $< 15\,\mathrm{K}$. Some SNSPDs are made of crystalline superconducting material and have slightly different performance and refrigeration

needs. Detectors fabricated with niobium nitride (NbN), for example, have a threshold temperature of $T_C \approx 10\,\mathrm{K}$ and therefore can be operated in a standard 4 K cryocooler (Verevkin et al., 2002).

The cryostat for our QKD receiver is a two-stage design comprised of a Gifford-McMahon (GM) style (Model RDK-101D with a Zephyr compressor) closed-cycle cryocooler from Sumitomo that has a base temperature just below 4 K. The GM cooler is used to pre-cool a single-stage sub-Kelvin ^{4}He cooler from Simon Chase Cryogenics with a base temperature $\sim 850\,\mathrm{mK}$. This cryostat is designed to support the operation of SNSPDs made out of tungsten silicide (WSi), molybdenum silicide (MoSi), and other amorphous superconducting materials that require sub-Kelvin operation for optimal performance.

Gifford-McMahon systems cool through rapid expansion of compressed helium gas. The high pressure helium gas is delivered by an external compressor unit to the a small volume that is in thermal contact with the sample mount. The compressed gas undergoes isothermal expansion and removes heat from the sample stage, which is then expelled in to the lab environment once it is delivered back to the compressor for re-cycling. Synchronized pistons in the compressor and coldhead control the timing of the gas flow to and from the coldhead. The coldhead is mounted to a vacuum flange and has cooling stages at 40 K, with 5 W of cooling power at 40 K, and 4 K with 200 mW cooling power at 4 K. Cooling data for the 4 K system is shown in Fig. 3.2a.

The Simon Chase cooler is a ^{4}He sorption fridge that holds a reservoir of helium gas and is mounted to the 4 K stage of the GM coldhead. The sorption fridge is pre-cooled to 4 K and a charcoal getter-pump holds the helium gas because of cryo-pumping. The pump is heated to release the captured helium and is subsequently re-liquified by bringing the pump in to thermal contact with the 4 K plate with a gas-gap controlled heat switch. The helium liquifies and flows to the 1 K sample plate

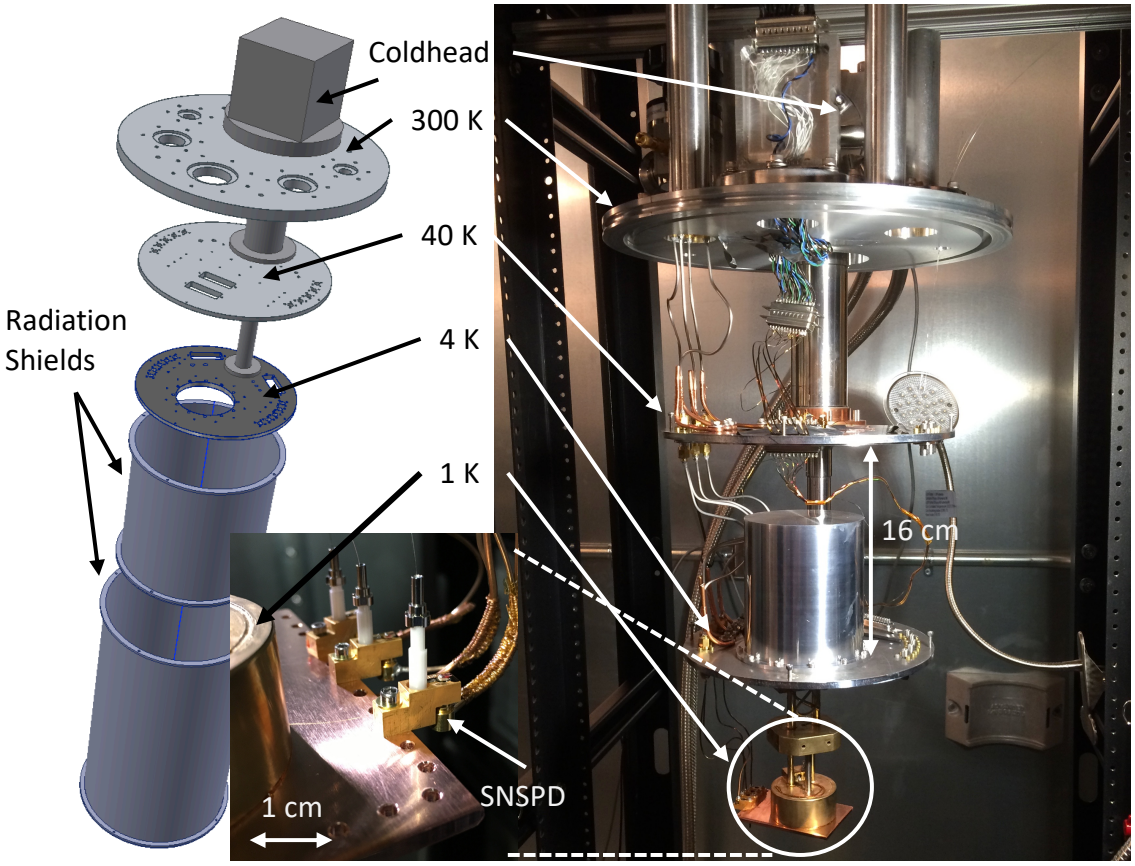

FIGURE 3.1: Cryostat exploded model view (left) and photograph of the assembled cryostat (right). Not shown in the right photograph are the 40 K and 4 K radiation shields. Not shown in either panel is the 300 K vacuum nipple. At the bottom of the photograph is the 1 K sample plate that is attached to the coldfinger of the Simon Chase sub-Kevlin cooler. SNSPDs mounted on the 1 K plate are shown in the inset.

where it boils off and cools the plate through evaporative cooling. The hold time of the 1 K plate is $35 - 45$ hours depending on the thermal load. Once the helium has been evaporated, the system must be re-cycled. The sub-Kelvin cooler has $100\,\mu$W of cooling power at 1 K. Cooling data for the 1 K system is shown in Fig. 3.2b.

The assembled system with an exploded model view is shown in Fig. 3.1. The coldhead mounts to a machined flange and is enclosed by a vacuum nipple which serves as a 300 K radiation shield and vacuum chamber. Vacuum is required to thermally isolate each temperature stage from heating by convection. The 40 K

and 4 K plates also have radiation shields to reduce radiative heating of the enclosed surfaces. The 300 K, 40 K, and 4 K sample plates and radiation shields were designed by Dr. Sae Woo Nam's group at the National Institute of Standards and Technology (NIST).

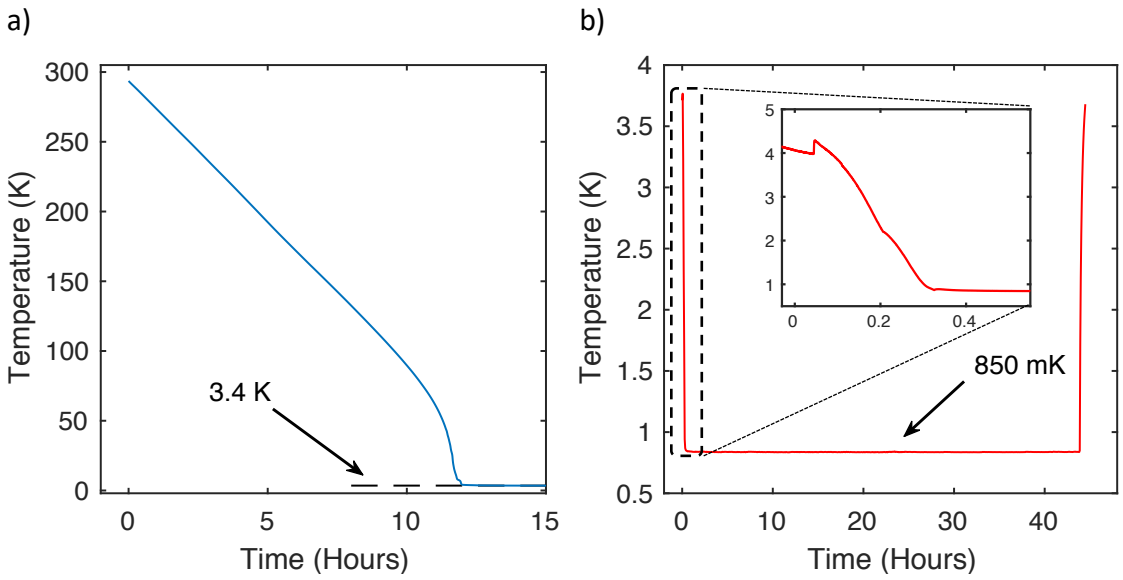

FIGURE 3.2: Cooling data for the GM 4 K cooler and 1 K sorption fridge. (a) Cool-down time for the GM 4 K cooler. The time to reach base temperature is a function of the thermal mass on the 4 K plate. With the 1 K system thermally anchored on this plate, this system takes $\sim$ 12 hours to cool to $<$ 4 K. (b) Typical 1 K hold-time with one detector operating. As the number of detectors (and therefore the number of thermal pathways from 4 K to 1 K) increase, the hold time will decrease. However, the hold time still remains $>$ 35 hours when multiple detectors are in operation. (Inset) Cooling time for the 1 K plate after the helium has been released from the charcoal getter.

3.2 Electrical and Optical Access

Detectors and other internal components such as temperature sensors and amplifiers are accessed through ports on the top 300 K plate. Direct-Current (DC) electrical access is provided by a D-subminiature 25-pin vacuum feed-through adapter on a KF-40 flange. These lines are used for temperature sensors, heaters, and provide

power to other internal electronics such as low-temperature amplifiers. Coaxial lines are accessed through hermetically sealed SMA feedthrough connections. These lines carry high-frequency detection signals from the detectors. Un-jacketed optical fibers provide optical access to the detectors through a vacuum feed-through port sealed with vacuum epoxy.

Low thermal conductivity materials are required for components such as DC wires and coaxial cables to minimize thermal loading of the colder stage by the warmer stage. A material's thermal conductivity is a function of temperature, and so care must be taken when making material choices for connections between each temperature stage. The DC wires are 32-AWG phosphor-bronze wires (Lakeshore Cryotronics QL-32) designed for cryogenic operation. These lines must be well-filtered from high-frequency electrical noise that can come from power supplies, measurement equipment, or signals radiated in the lab environment. The DC feedthrough is filtered in three stages. First, a commercial D-subminiature low-pass filter attenuates high-frequency noise down to $\sim 5\,\mathrm{MHz}$. Second, a capacitive filter attenuates frequencies in the range of $\sim 1 - 10\,\mathrm{MHz}$. Lastly, a home-made 5-pole, 3 dB ripple, Chebyshev low-pass filter attenuates signals above $\sim 275\,\mathrm{kHz}$. These filters provide clean electrical lines for sensitive measurements and readout electronics, shown in Fig. 3.3.

Two types of semi-rigid coaxial cables that carry high-frequency electrical signals are used in our cryostat. Beryllium-copper outer conductor and silver-plated beryllium-copper inner conductor cables (Coax Co. LTD SC-119/50-SB-B) carry detection signals from the SNSPD on the 1 K stage to the 4 K stage. Stainless steel (304) outer conductor and silver-plated beryllium-copper inner conductor cables (MicroCoax UT-085B-SS) carry detection signals from 4 K to 40 K, and from 40 K to 300 K. Stainless steel and beryllium-copper have low thermal conductivity (approximately 0.3 W/m-K and 2 W/m-K respectively at 4 K and 3 W/m-K and 11 W/m-K

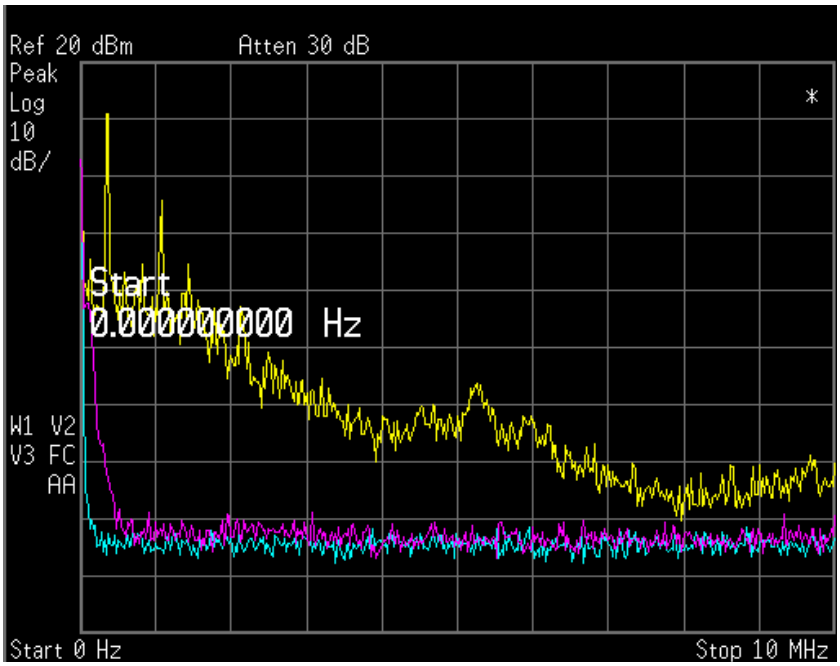

FIGURE 3.3: Spectrum analyzer traces of noise data before and after filtering. The domain of the scan is from DC to 10 MHz and the vertical scale is 10 dB/division. The signals plotted include $\sim$ 30 dB of amplification in order to make them visible above the noise floor. The blue trace is the baseline spectrum, the yellow trace is the spectrum with no filtering, and the pink trace has low-pass filtering down to 275 kHz.

at 40 K) and silver-plating on the inner conductor reduces high-frequency electrical loss.

3.3 Superconducting Nanowire Single-Photon Detectors

The first superconducting nanowire detector was realized at the University of Moscow by Gol'tsman and colleagues (Semenov et al., 2001) with a 225-nm-wide, 1-μm-long niobium nitride wire operating at 4.2 K. Optical photon detection was demonstrated at a bias current of 70 μA. Advancements in fabrication and packaging techniques have been developed by several groups to improve optical coupling (Miller et al., 2011), increase detection efficiency (Rosenberg et al., 2004; Rosfjord et al., 2006), investigate alternate superconducting materials (Baek et al., 2011; Verma et al.,

2014b, 2015), and develop complex detector structures including pixel arrays (Dauler et al., 2009; Verma et al., 2014a; Allman et al., 2015) and parallel elements (Najafi et al., 2012; Zhao et al., 2014). These advancements and recent demonstrations of high detection efficiency (Marsili et al., 2013), high maximum count rate (Kerman et al., 2006) and good timing resolution (Zadeh et al., 2017), have enabled SNSPDs to be a leading commercial technology (Photon Spot, Inc., Single Quantum, Quantum Opus, LLC) for quantum optics experiments.

To understand the amplifier design discussed in the Chapter 4, we highlight the important operating characteristics of the SNSPD. In the detector quiescent state, a superconducting nanowire cooled to below T_C carries a constant bias current $I_{bias} < I_{sw}$ without resistance, where I_{sw} is the switching current for the device. If I_{bias} exceeds I_{sw} then the detector will become unstable or fall in to a resistive state, referred to as latching. A photon absorbed in the nanowire deposits energy causing Cooper pairs to break, locally disrupting the superconductivity to create a resistive region, referred to as a hot-spot. The hot-spot method is used here, as opposed to other detection theories discussed elsewhere (Bulaevskii et al., 2012; Gaudio et al., 2016). The temperature of the hot-spot region grows due to Joule heating and the resistive region grows due to diffusion and non-equilibrium quasi-particles (Semenov et al., 2001; Renema et al., 2014) until a short section of the wire is resistive. The value of the hot-spot resistance depends on the material, nanowire geometry (Kerman et al., 2006), electrical readout circuit (Kerman et al., 2009), and likely indicates the number of absorbed photons (Cahall et al., 2017; Nicolich et al., 2018). Photon-number resolution is discussed in more detail in Chapter 5. As the hot-spot resistance grows current through the device is reduced, and after some amount of time the size of the hot-spot stagnates and cooling through the substrate starts to dominate until the detector has cooled sufficiently to become superconducting again. The value of resistance for an individual hot-spot R_{hs} can

range from $500\,\Omega - 5\,\mathrm{k}\Omega$. The growth and stagnation of a photon hot-spot is on the order of a few hundred picoseconds (Semenov et al., 2001; Engel et al., 2015; Marsili et al., 2016).

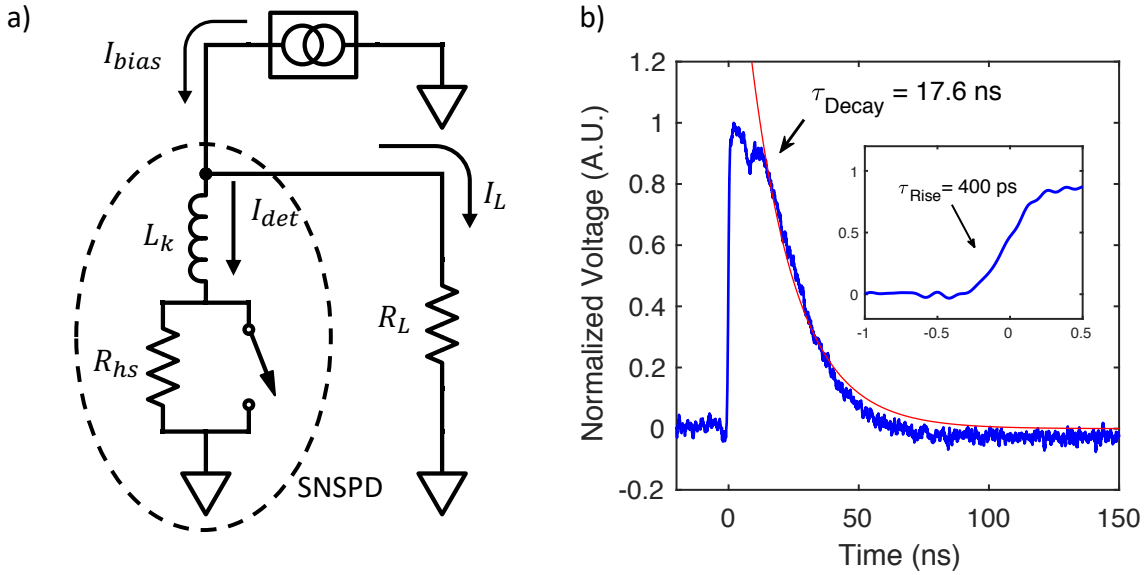

FIGURE 3.4: Simple SNSPD circuit and photon detection waveform. (a) Simple SNSPD circuit model. The switch begins in a closed position to represent the detector in a superconducting state with a DC bias current I_{bias} flowing unimpeded through the device. A photon is absorbed and the switch opens. Current is diverted out of the device and in to the load resistor R_L. (b) A single-shot detection waveform from an amorphous SNSPD having a meander diameter $\sim 15\,\mu$m. This pulse is amplified by two low-noise room-temperature amplifiers (Miteq AU-1310). The waveform decay time $\tau_{Decay} = 17.6\,\mathrm{ns}$ and load impedance $50\,\Omega$ gives a kinetic inductance value $L_k = 875\,\mathrm{nH}$. (Inset) Rising edge of a single-shot detection waveform recorded with a 2.5 GHz bandwidth cryogenic amplifier (Cosmic Microwave Technologies CITLF3). The value $\tau_{Rise} = 400\,\mathrm{ps}$ gives a hot-spot resistance value $R_{hs} \approx 2\,\mathrm{k}\Omega$.

In the lumped-element circuit picture, the SNSPD is modeled as an inductor L_k in series with a resistor R_{hs} to ground, as shown in Fig. 3.4. The bias current provided by the source is I_{bias} and the current flowing through detector is I_{det}. The nanowire begins in a superconducting state, and so the switch in parallel with the resistor is closed and I_{det} is equal to I_{bias}. A photon detection event corresponds to the switch opening, leading to the detector resistance R_{hs}. Bias current is diverted out of the

detector in to a parallel resistor R_L, typically the 50 Ω input impedance an amplifier, and the shunted current I_L is detected as an output pulse. The reduction in I_{det} allows the detector to cool down and the nanowire to return to the superconducting state, closing the switch. The rise time of the detected pulse is determined by $\tau_{Rise} \approx L_k/R_{hs}$, and the recovery time for the pulse to fully decay and the detector to reset is determined by $\tau_{Decay} \approx L_k/R_L$. The inductance arises from the kinetic inductance of the superconducting nanowire. The values for L_k and R_{hs} are estimated using each of these time-constants of the detection waveform. The value for L_k is estimated by fitting an exponential function to the recovery of the waveform falling edge using the value for the read-out circuit load resistance, such as a 50 Ω room temperature amplifier. Once L_k is known, the value for R_{hs} is estimated by measuring the rise-time of a detection waveform. A high bandwidth read-out must be used in order to reduces the effects that a bandwidth-limited read-out circuit has on the fast rising edge of the waveform. In the device and read-out circuit that is discussed in the following chapters, $L_k \approx 875$ nH and $R_{hs} \approx 2$ kΩ.

3.4 Conclusion

In this chapter I have given a description of the infrastructure needed to realize a high performing quantum receiver. The central component to the receiver design is a superconducting nanowire single-photon detector. SNSPDs must operate at cryogenic temperatures and therefore necessitate the construction of a cyrostat system. Our system is two-stage system comprised of a closed-cycle 4 K cooler that pre-cools a ^{4}He sorption fridge with a base temperature of 850 mK. This is suitable for the operation of SNSPDs made from amorphous superconducting material. The cryostat is also outfitted with the necessary access include DC and RF electrical connections and optical fiber access to carry photons to the detectors. I conclude the chapter by describing the operating principles of SNSPDs.

4

Cryogenic Amplifiers

Chapter 3 introduced the necessary hardware needed to build a quantum communications receiver. This chapter discusses the optimization of the receiver for the high-rate QKD protocol discussed in Chapter 2, featuring the development of novel, cryogenic amplifiers.

Critical detector characteristics, such as timing resolution (Wu et al., 2017), reset times (Kerman et al., 2006) and maximum count rates (Kerman et al., 2013), are often dictated by the read-out electronics that sense and amplify the electrical signal generated in response to a photon detection event. This chapter describes the design and performance of cryogenic amplifiers that provide two critical advantages for SNSPD read-out: (1) the intrinsic amplifier noise can be reduced dramatically, improving the signal-to-noise ratio (SNR) and hence the timing resolution; and (2) placing the first-stage preamplifier closer to the device provides flexibility to design the effective load impedance of the amplifier with minimal signal loss between the detector and the preamplifier. There have been recent demonstrations of low-noise, low-power cryogenic amplifiers built from custom-made components (Bardin and Weinreb, 2009; Montazeri et al., 2016) and commercially available transistors (Mani

and Mauskopf, 2014). The main goal of our effort is to identify a commercial monolithic amplifier read-out circuit that maximizes timing resolution while maintaining high count rate capabilities, and scalability in terms of cost and power consumption. These characteristics have a significant impact on the speed and fidelity of quantum communication protocols such as time-phase QKD (Brougham et al., 2016).

A read-out circuit optimized for timing resolution and maximum achievable count rate is low noise, has a large bandwidth, and is DC coupled at the amplifier input. Electrical read-out noise is the dominant contribution to the timing uncertainty and is approximately quantified by the rise time of the photon detection waveform divided by the SNR (Marsili et al., 2013). Timing performance is improved by a reduction in the amplifier noise and securing a large bandwidth to improve the rise time of the photon detection waveform. The relaxation time of a photon hot-spot is on the order of $\sim 500\,\mathrm{ps}$ (Marsili et al., 2016) and so a bandwidth of a few GHz is desired.

We explore a range of read-out-circuit strategies using commercial gallium arsenide (GaAs) monolithic microwave integrated circuits (MMIC) and silicon germanium (SiGe) operational amplifiers (Op-Amp). Unlike conventional silicon devices, GaAs and SiGe chips do not suffer from carrier freeze-out at cryogenic temperatures, and provide a viable solution for the SNSPD read-out circuit. Amplifier prototypes are assembled on patterned Rogers 4003C high frequency printed circuit board (PCB) with passive components selected for cryogenic compatibility, such as thin film resistors (Lamb, 2014) and ceramic capacitors using C0G/NP0 dielectric (Teyssandier and Prêle, 2010). The amplifier consists of bias circuitry for powering the amplifier chip as well as a custom bias network used to split the DC current bias to the detector and the high-frequency detection signal at the amplifier input. The detector used for the characterization of these read-out circuits is made of a proprietary amorphous superconducting material from Quantum Opus and has a critical temperature $T_C \approx 5\,\mathrm{K}$, a threshold current $I_{sw} = 13.5\,\mu\mathrm{A}$, and kinetic inductance $L_k \approx 875\,\mathrm{nH}$.

The efficiency of this detector is optimized at $\sim 1\,\mu$m wavelength. The detection efficiency as a function of bias current measured at 1550 nm is shown in Fig. 4.1. When operated with standard room temperature amplifiers this detector has a $1/e$ recovery time of 17.6 ns, a rise time of ~ 700 ps, and an SNR of ~ 28. The detector is operated in the cryostat discussed in Chapter 3 where the 4 K-stage of the GM cryocooler provides sufficient cooling power (200 mW at 4.2 K) for thermally anchoring the low temperature pre-amplifiers.

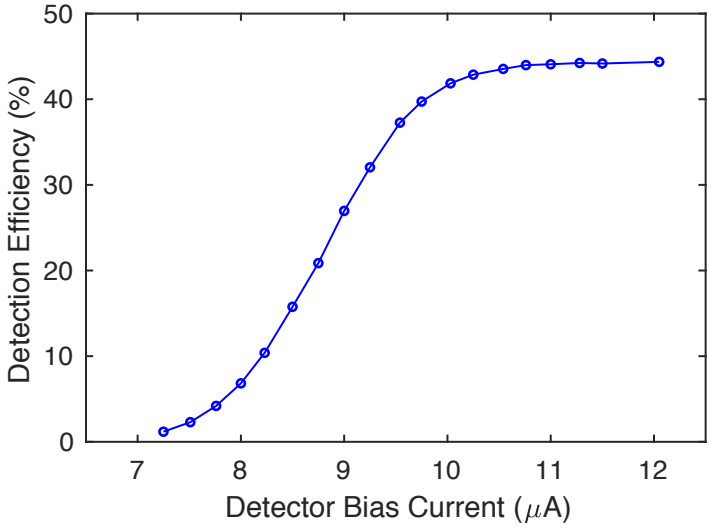

FIGURE 4.1: Detection efficiency of the detector used in our amplifier study, measured at 1550 nm.

4.1 SiGe Op-Amp Read-out

A non-inverting amplifier utilizing SiGe op-amps is a natural choice for a DC-coupled read-out scheme. Specifically, the high input impedance of the non-inverting input gives the freedom to tune the load resistance by adding an external shunt resistor. Increasing the load resistance decreases the recovery time of the detector, given by L_k/R_L. The value of R_L is restricted to a maximum value of $200 - 250\,\Omega$ before the

detector is prevented from self-reseting (Yang et al., 2007). The gain of the amplifier is easily control by adjusting the feedback circuit. Our non-inverting amplifier design uses a SiGe Op-Amp from Texas Instruments (LMH6629), and the circuit configuration is shown in Fig. 4.2. A bias resistor $R_{bias} = 100\,\mathrm{k}\Omega$ provides a constant bias current to the detector. A small resistor $R_{In} = 20\,\Omega$ is needed on the non-inverting input for offset bias current cancellation in the op-amp and the ratio of the feedback resistor R_F to the gain resistor R_G determines the gain of the amplifier. Our amplifier prototype has $\sim 13\,\mathrm{dB}$ of gain with a $\sim 300\,\mathrm{MHz}$ 3 dB bandwidth. The performance of this read-out scheme is shown in Fig. 4.3a.

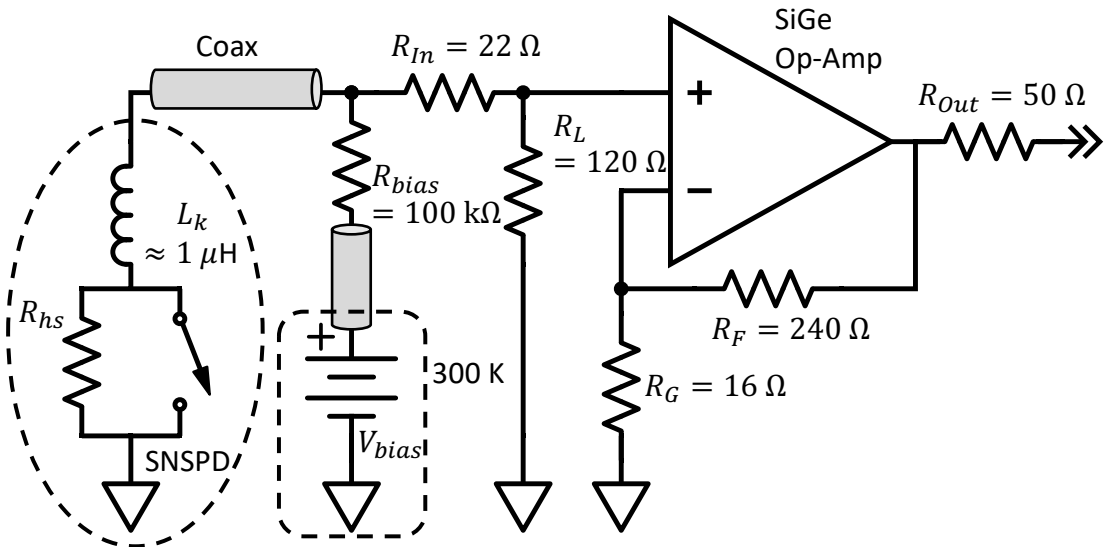

FIGURE 4.2: Simplified schematic of the SiGe Op-Amp in a non-inverting setup coupled to the SNSPD.

The SiGe Op-Amp readout scheme features a fast recover time of 11.9 ns, enabling maximum count rates approaching 85 million counts-per-second (Mcps). Additionally, the SNR of the detection waveform with this read-out scheme is ~ 100, a more than factor of three increase compared to room temperature amplifiers. However, the small bandwidth limits the rise-time of the detection waveform to $\sim 3.5\,\mathrm{ns}$, ap-

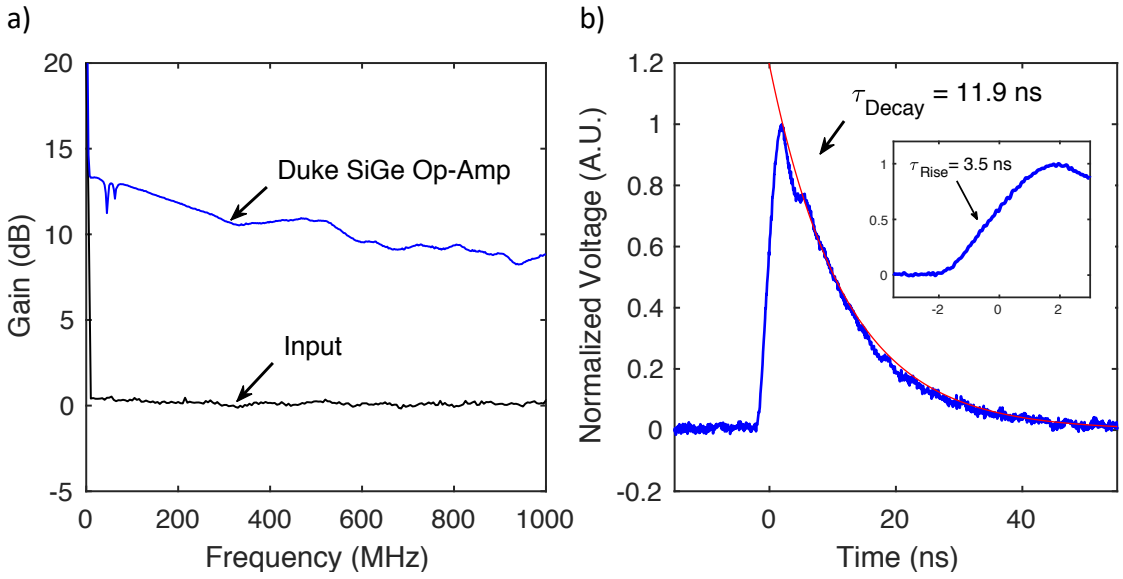

FIGURE 4.3: Performance characterization of the SiGe Op-Amp. (a) Op-Amp gain spectrum is measured using the tracking source of a spectrum analyzer as the input (shown in the black trace for reference). The output of the amplifier is shown in the blue trace. (b) Single-shot detection waveform. The waveform is recorded using the SiGe Op-amp and a low-noise room temperature amplifier (Miteq AU1310). The waveform decay $\tau_{Decay} = 11.9\,\text{ns}$ is 30% shorter compared room temperature amplifiers due to the increased load impedance. (Inset) Rising edge of the detection waveform.

proximately a factor of five slower than the rise time measured with typical room temperature amplifiers for this detector. The rising edge of the detection waveform is shown in Fig. 4.3b. As a result of the slow rising edge, the timing resolution of this read-out scheme is diminished and offers little to no improvement over low-noise room temperature amplifiers. Details about timing-resolution measurements are discussed later in this chapter.

Ultimately, this read-out scheme was not a good candidate for a high-rate communication demonstration because of its poor timing resolution, despite having a good SNR and a short recovery time. However, this scheme was useful for achieving a high detection rate where precise timing resolution is not critical, such as state-dependent fluorescence in a trapped atomic ion (Crain, 2016; Crain et al., 2019).

4.2 GaAs MMIC Read-out

Our most successful circuit uses a GaAs MMIC amplifier chip from Broadcom Limited, formerly Avago Technologies (MGA-68563). A schematic of the detector and GaAs MMIC read-out circuit is shown in Fig. 4.4. Our amplifier has a 1.5 GHz bandwidth, gain of 15 dB at room temperature, and a 65 K noise temperature measured at 4 K. The noise temperature is measured at a frequency of 100 MHz (well within the high-pass band of the L-R filter, explained later in this chapter) using the Y-Factor Method (Horowitz and Hill, 1989). We compare the GaAs MMIC read-out circuit to the high-performance cryogenic amplifier CITLF 3 built by Cosmic Microwave Technology, formerly part of the Microwave Research Group at California Institute of Technology. The CITLF 3 features 30 dB gain over a bandwidth of 2.5 GHz, a noise temperature of 4 K, dissipates 24 mW of power, and carries a high cost. We also compare our results to the performance of commercial low-noise room-temperature amplifiers (Miteq AU1310).

The gain spectra of the GaAs MMIC circuit and the CITLF 3 amplifier, both measured at 300 K, are shown in Fig. 4.5a. One distinct advantage of our circuit is the low power dissipation compared to commercial cryogenic amplifiers. We measure power dissipation of the amplifier operating at a temperature of 4 K by recording the supplied current at different bias voltages. As the bias voltage increases, the amplifier gain increases as well as the signal height. The SNR measured at 4 K is calculated from the average peak height compared to the variance of the noise floor. The SNR improves as power is dissipated by the amplifier. The SNR levels off at ~ 115 with ~ 3 mW dissipated, shown in Fig. 4.5b. All subsequent measurements for the GaAs MMIC circuit are performed at this bias point of the amplifier. When compared to the 24 mW dissipated by the CITLF 3 amplifier, an order-of-magnitude reduction in power consumption in our amplifier allows multiple channels to operate

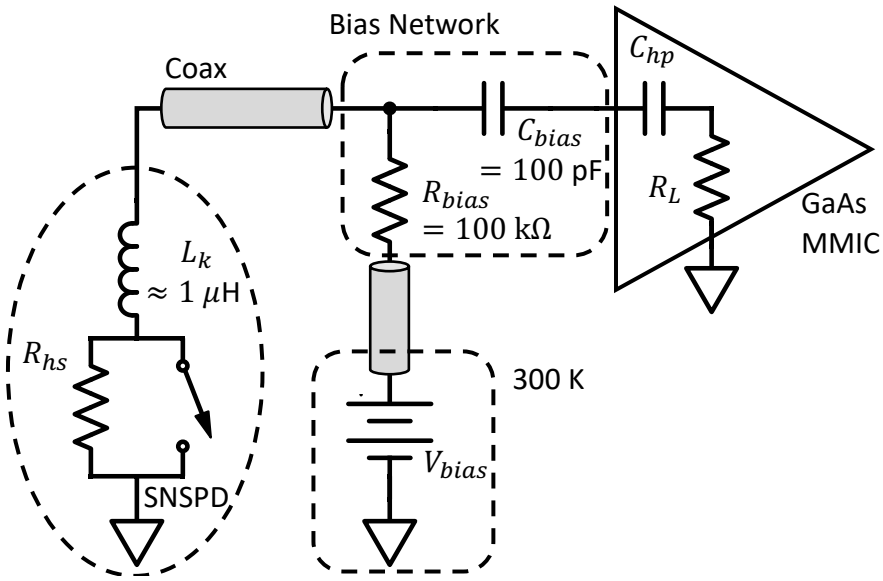

FIGURE 4.4: Simplified circuit schematic of the detector and GaAs MMIC amplifier setup (Cahall et al., 2018). The bias-network on the amplifier front-end has component values $C_{bias} = 100\,\text{pF}$ (Vishay Vitramon, P/N: VJ0603A101KXBAC31) and $R_{bias} = 100\,\text{k}\Omega$ (Susumu, P/N: RR1220P-104-D). The resistor in the bias-network has a large value to act as a constant current source. The high-pass corner frequency and input impedance are set by the series capacitor C_{hp} and resistor to ground R_L. These components are internal to the amplifier and their values depend strongly on the operating temperature.

simultaneously without overloading the cryogenic system.

The GaAs MMIC chips are not designed to operate at cryogenic temperatures and so their performance drastically changes when cooled to 4 K. As shown in Fig. 4.6a, the waveform observed for photon detection events consists of decaying oscillations with an oscillation frequency of $\sim 20\,\text{MHz}$ and an exponential decay time of $\tau_{Decay} \sim 193\,\text{ns}$, which is $10\times$ longer than expected for an input load resistance of $50\,\Omega$. This indicates that the load resistance R_L of the amplifier decreases substantially below its room temperature value of $50\,\Omega$ when it is cooled.

To confirm this behavior, we fit the data shown in Fig. 4.6a to the predictions of a PSpice model where we adjust the value of R_L and C_{hp} to match the data. The circuit simulations are performed with the following assumptions: the short coax

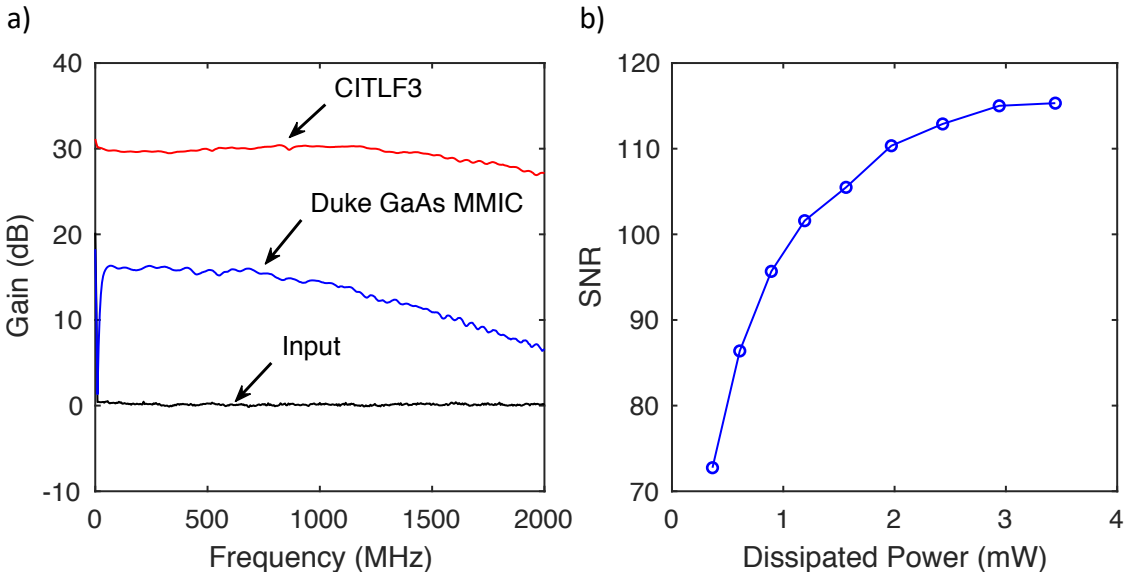

FIGURE 4.5: Performance characterization of GaAs MMIC read-out scheme (Cahall et al., 2018). (a) Gain spectra are measured using the tracking source of a spectrum analyzer as the input (shown in the black trace for reference). The output of the CITLF 3 amplifier and the GaAs MMIC circuit are shown in the red and blue traces respectively. (b) SNR of photon detection waveforms recorded at a detector bias current of 12 μA as a function of the dissipated power of the GaAs MMIC amplifier.

transmission line between the detector and the amplifier is assumed to be lossless, traces on the PCB that are smaller than 2 cm are not treated as transmission lines in simulations, and the input of the amplifier is simplified as a high-pass capacitor C_{hp} with a load resistor R_L as shown in Fig. 4.4. Our model reveals an under-damped LRC resonator, formed by the kinetic inductance of the detector L_k, the input capacitance of the amplifier C_{hp}, and load resistance of the amplifier R_L. This analysis reveals that $R_L \sim 5 - 10\,\Omega$ and $C_{hp} \approx 33\,\text{pF}$.

The input stage of the amplifier, and the load resistor in particular, is not accessible and so we add an external circuit to modify the effective load impedance and mitigate the slowly decaying oscillations. A slow decay of the photon detection waveform limits the maximum achievable count rate, and therefore a slow decay is unwanted. In order to mitigate this effect and maintain high SNR and maximum

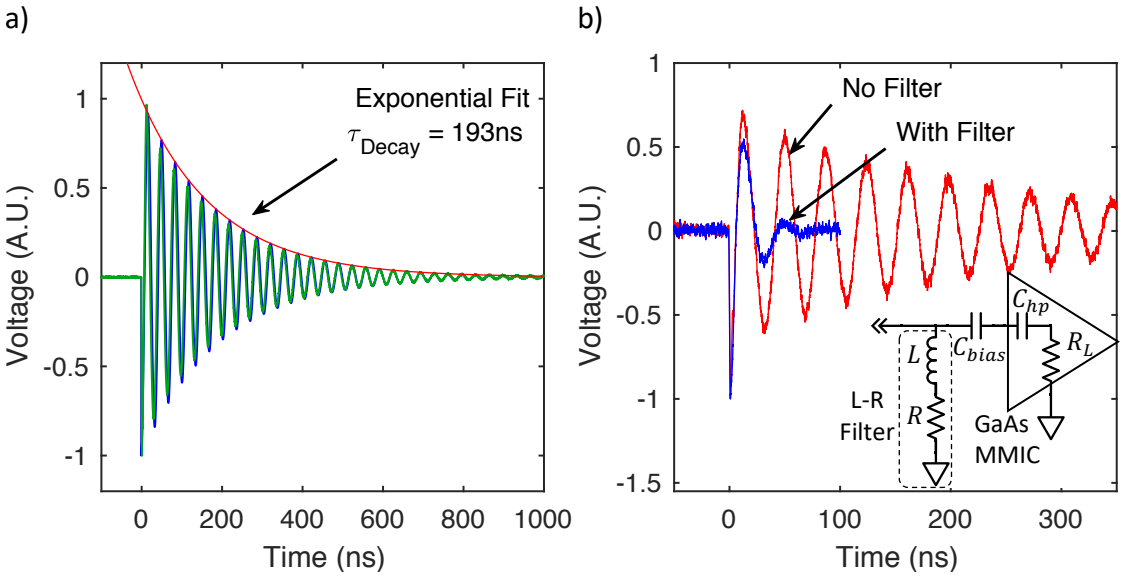

FIGURE 4.6: Photon detection characterization of GaAs MMIC read-out scheme with an SNSPD (Cahall et al., 2018). (a) Detection event waveform (average of 64 traces, green) compared to our PSpice circuit model (blue). The decay time is 10x longer than expected for a 50 Ω load, indicating that the input resistance of the amplifier chip changes significantly when cooled to 4 K. (b) Filtered single-shot photon pulse compared to an unfiltered single-shot pulse. The $1/e$ recovery time τ_{Decay} is reduced by an order-of-magnitude, while the rise time and SNR are maintained. (*Inset*) Amplifier circuit schematic showing the L-R filter. The frequency band of the L-R path to ground is chosen to include the oscillation frequency. In our circuit $L \sim 220$ nH (Epcos, P/N: B82496C3221J000) and $R \sim 100\,\Omega$ (Susumu, P/N: RR1220P-101-D).

bandwidth, we add a L-R high-pass filter to the read-out circuit that performs multiple functions. First, it creates a path to ground for all frequencies between DC and its 3-dB cut-off frequency given by $R/2\pi L$. Here, this cut-off frequency is chosen so that the oscillations observed in Fig. 4.6a are coupled to ground and hence not to the amplifier. An L-R filter with the values $L = 220$ nH and $R = 100\,\Omega$ is used in the measurements discussed in the following section. Second, it provides a DC path to ground to prevent reverse biasing of the detector at high photon detection rates, as discussed below. Figure 4.6b shows the photon-detection-event waveform with the filter, where it is seen that the damping time is so short that only a single

oscillation cycle is observed. In the context of a quantum communications system with a time-bin encoding (Islam et al., 2017a) the waveform with the filter in place is acceptable for reliably resolving photon detections at a rate of $\sim 25 \times 10^6$ counts per second. The amplifier design discussed in this section is used in a high-rate QKD demonstration (Islam et al., 2017b,a), described in more detail at the end of this chapter.

4.3 Maximum Count Rate

The maximum achievable count rate (measured in million counts per second, or Mcps) is a performance metric that is heavily influenced by the read-out circuit. The largest contributing factor to the maximum count rate is the input coupling of the first amplifier. As described in Kerman et al. (2013), AC-coupled read-out schemes lead to detector saturation at low detection rates due to self reverse biasing of the detector. This effect, due to charge build-up on the input capacitor in the AC-coupled scheme, is present when the detection rate approaches even a small fraction of the detector recovery time. The high-pass filter employed in our setup (Fig. 4.6b) provides a DC path to ground other than through the detector itself, avoiding this problem. The room temperature amplifier and CITLF 3 are AC-coupled, and hence are expected to have degraded saturation characteristics.

We measure the observed count rate as a function of the input optical power with the setup shown in Fig. 4.7a. Saturation results in a slower-than-linear count rate as a function of the input power because photons arrive at the detector during the deadtime of the detector. As discussed previously, the deadtime of the detector is determined by $\tau_{Decay} = L_k/R_L$. The dependence of τ_{Decay} on the load resistor implies that the read-out circuit will effect the maximum count rate of the detector (Yang et al., 2007; Kerman et al., 2009, 2013). We measure the maximum count rate on a single-pixel, amorphous SNSPD with continuous-wave laser light at 1550 nm

(Wavelength Reference, Clarity-NLL-1550-HP) and a time-tagger (Agilent, Acqiris U1051A). Input flux to the SNSPD is inferred from the measured power reference and a careful calibration of the attenuation in the path to the detector. Our results are shown in Fig. 4.7b-c.

In our GaAs MMIC read-out scheme, the detector operates at a constant bias current of 12 μA and the measured counts increase linearly at low input flux until saturation effects become appreciable at the input photon rate of 2 Mcps. The line continues to track smoothly and reaches a maximum measured count rate just above 20 Mcps. This is the point where our time-tagger began dropping significant counts.

The room temperature amplifier scheme closely follows that observed with the GaAs MMIC circuit until a measured count rate of $\sim$ 10 Mcps. To obtain these results with the room temperature amplifier, we had to adjust the detector bias above an input flux of 1 Mcps to compensate for the current back-action and prevent the detector from latching. The measured counts decrease rapidly at a measured count rate of $\sim$ 10 Mcps due to a reduction in the detector bias current to a level such that the efficiency of the detector is decreased substantially.

The detector saturation characteristics using the CITLF 3 read-out circuit is measured with and without a 3 dB electrical attenuator at the amplifier input. Without the attenuator, the AC-coupled input to the amplifier causes the detector to latch at a much lower bias current. This latching behavior is worse than that observed with the room temperature amplifier. We believe that the difference between the latching behavior of these two AC-coupled schemes is due to the proximity of the amplifier input to the detector, or to differences in the input circuit between the two amplifiers. Due to the lack of a DC path to ground, the detector bias current had to be adjusted to compensate for latching at each data point. The reduction in bias current is the cause for the poor efficiency. A 3 dB attenuator installed between the detector and the amplifier provides a DC path-to-ground. In this case, we measure the detector

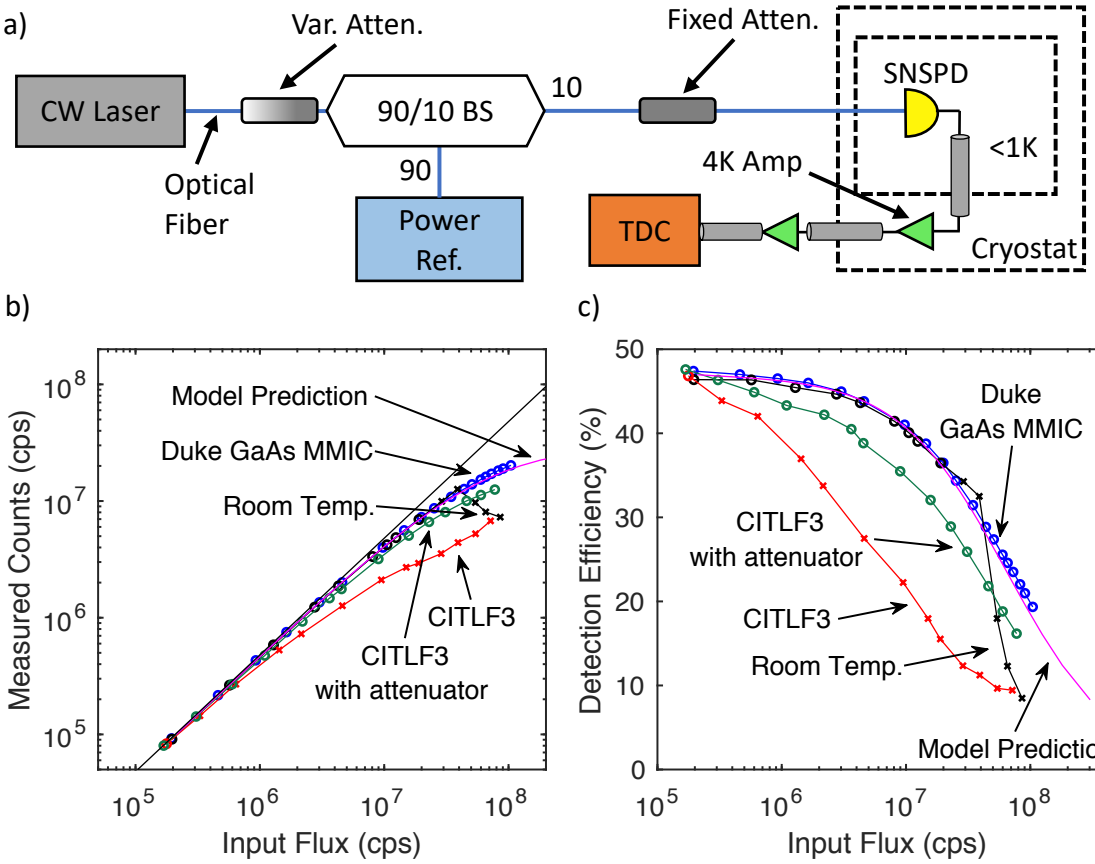

FIGURE 4.7: Maximum count rate measurement using different amplifier read-out schemes (Cahall et al., 2018). (a) Experimental setup for measuring the maximum count rate. (b) Measured count rate as a function of the input optical flux. The black line shown is a fixed efficiency of 48%, which is the expected value at 1.55 μm for this device optimized for operation at a wavelength of 1 μm. The purple line shows the expected count rate for a 50 Ω load resistance as predicted by Kerman et al. (2013). The poor performance of the CITLF 3 without the attenuator is caused by premature latching of the detector due to the amplifier's AC-coupling. Data points with circles are recorded at a 12 μA detector bias current. Data points with X's are recorded at a reduced detector bias current due to the detector latching. (c) Count rate data in panel (b) plotted as an effective detection efficiency as a function of the input flux. As the input rate is increased, photons impinge more frequently on the detector before it has fully recovered and do not register a count, leading to a reduction in the detection efficiency.

saturation characteristics with a constant detector bias current of 12 μA. As shown in Fig. 4.7, the 3-dB attenuator substantially improves the counting capabilities of this read-out scheme. The reduction in measured counts when compared to GaAs MMIC

and room temperature amplifiers is hypothesized to be the result of a difference in the resistance to ground between our L-R filter on our GaAs MMIC circuit and that of the attenuator with the CITLF 3.

There are other possible front-end circuits that can be placed in front of the CITLF 3 amplifier to improve its saturation characteristics. For example, a custom L-R filter inserted between the amplifier and detector should improve the count rate capabilities of the CITLF 3 read-out scheme while providing a DC path-to-ground and avoiding signal attenuation as with the 3 dB attenuator used here. We believe the count rate performance of the CITLF 3 amplifier with an L-R filter could potentially closely follow the saturation characteristics observed for the GaAs MMIC circuit.

4.4 Timing Performance

The maximum rate of communication, especially in time-bin encoded protocols, is affected by the timing resolution of the detection system. We measure the timing resolution of our detector-readout circuit combination using a mode-locked pulsed laser source that emits a train of $\sim$ 5-ps-width pulses with a repetition rate of 75 MHz at a wavelength of 1030 nm. A schematic of the measurement setup is shown in Fig. 4.8a. The output beam is split by a polarizing beam splitter (PBS), and one beam is measured with a fast photodiode (Miteq DR-125G-A) that has a bandwidth of 12.5 GHz and a jitter of < 5 ps to serve as a stable timing reference for the pulse arrival. The other beam is heavily attenuated to the single-photon level and the attenuation of the path is adjusted so that the detection rate is $\sim$ 100 kcps (mean photon number $\sim 10^{-3}$ per pulse). The timing resolution of the fast photodiode is verified by using two identical photodiodes and recording the timing resolution of one while the other is used as the timing reference. The measured timing resolution the resolution of each detector added in quadrature.

A time-correlated, single-photon counting (TCSPC) module (PicoQuant Pico-

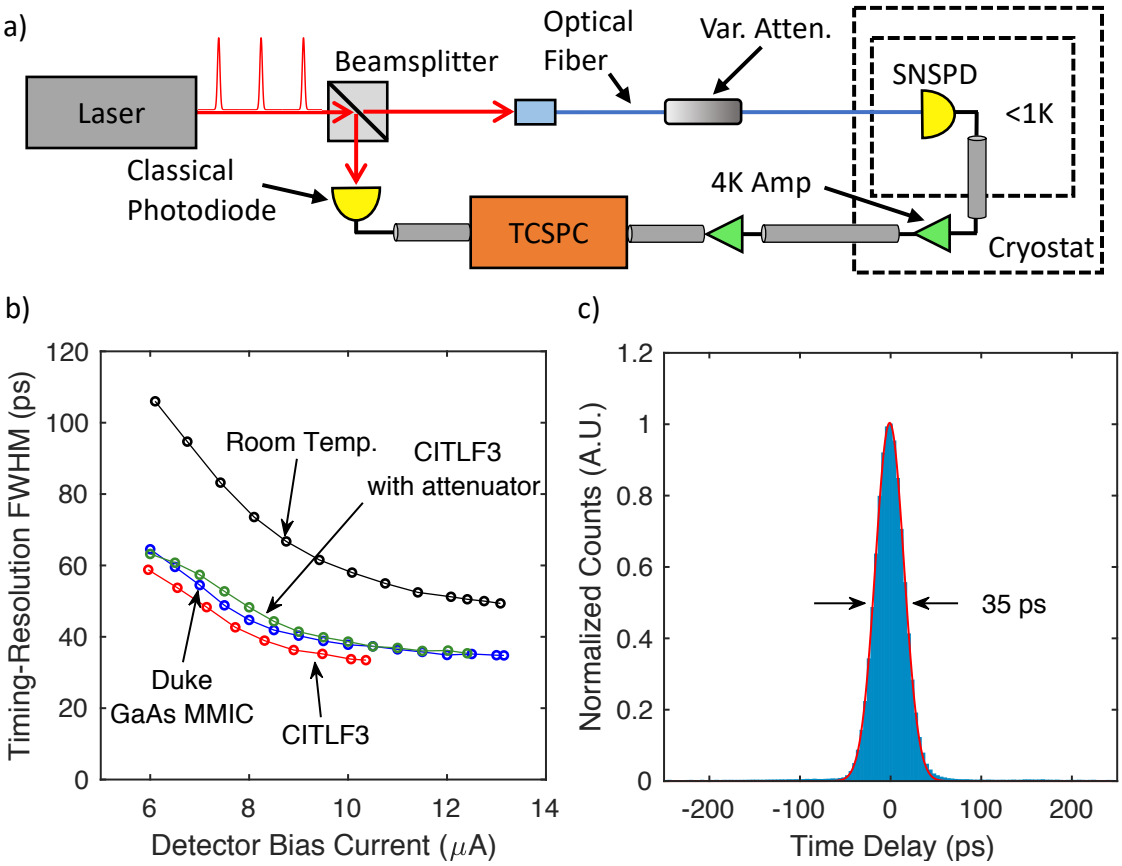

FIGURE 4.8: Detector timing resolution using different amplifier read-out schemes (Cahall et al., 2018). (a) Experimental setup for measuring the timing jitter of the photon detection. The time-correlated single-photon counting (TCSPC) module measures the time delay between the reference signal generated by the high-speed classical detector and the single-photon detection signal to build a time-of-arrival histogram. The full-width at half-maximum (FWHM) value of the Gaussian fit to this distribution characterizes the timing resolution of the system. (b) Timing-resoltuion as a function of detector bias current for different read-out schemes. (c) Time-of-arrival histogram recorded using our GaAs MMIC read-out scheme at a bias current of 13.1 μA. A Gaussian fit to the distribution is shown in the red line.

Harp 300) measures the time delay between the reference signal and the single-photon signal. The delay due to optical and electrical path length differences is adjusted so that the single-photon event comes after the reference event. We then record a time-of-arrival histogram, where the full-width at half-maximum (FWHM) of a Gaussian fit to the distribution characterizes the timing jitter of the detection system. The

timing performance of the GaAs MMIC scheme is compared to both the CITLF 3 amplifier and low-noise commercial room temperature amplifier. The results of our measurements are shown in Fig. 4.8b-c.

Low-noise room temperature amplifiers are the standard read-out scheme for SNSPDs and the timing performance of this scheme is a comparison benchmark for the other read-out schemes. The best timing resolution for room temperature amplifiers is 50 ps at a detector bias current of 13.1 μA. The CITLF 3 achieves the best timing performance at each detector bias current and reaches a minimum value of 33.5 ps at a detector bias current of 10.4 μA. A higher bias current was not accessible due to the detector latching. Adding the attenuator before the CITLF 3 enables a higher achievable count rate but it also degrades the photon detection signal and negatively influences the timing resolution. The addition of an L-R filter between the CITLF 3 and the detector in place of the 3 dB attenuator would provide a DC path-to-ground without degrading the detection signal. We believe the performance of the CITLF 3 read-out scheme with an L-R filter would be better than with the 3 dB attenuator and should closely follow the measurement without the attenuator. The timing resolution of the GaAs MMIC read-out circuit very closely follows the performance of the CITLF 3 amplifier with the attenuator on the input, and has a minimum FWHM value of 35.0 ps at a bias current of 13.1 μA.

4.5 High-Rate QKD Demonstration Results

The work in this section is done in collaboration with Dr. Nurul T. Islam, Dr. Charles C. W. Lim, and Prof. Daniel J. Gauthier. Dr. Islam constructed the transmitter. I assisted Dr. Islam in coupling the transmitter to the receiver, optimizing the system, and collecting preliminary data. Dr. Islam collected the published data (Islam et al., 2017a), performed the data analysis, and did the security proof with contributions from Dr. Lim.

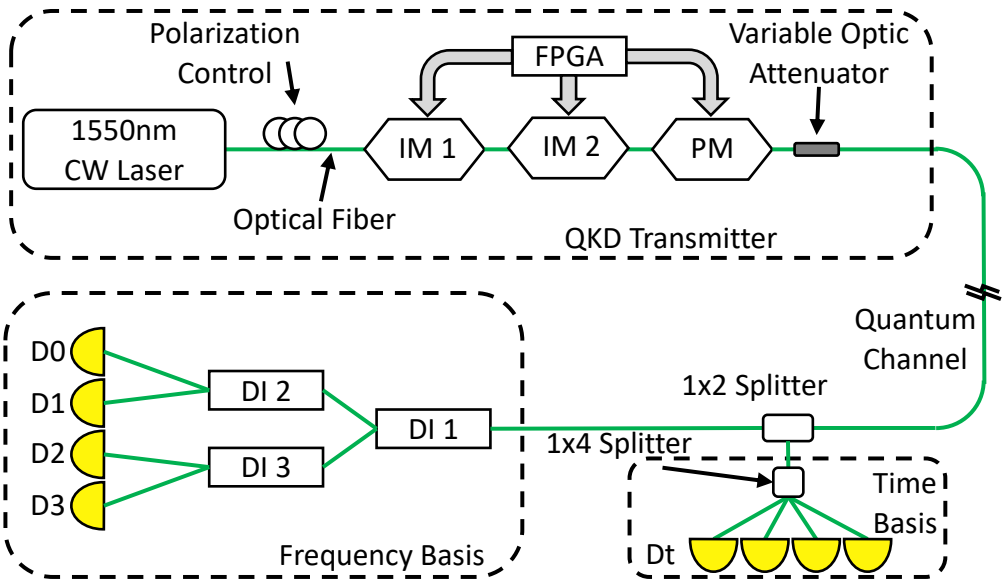

FIGURE 4.9: Experimental setup for the time-bin encoded QKD demonstration (Islam et al., 2017a).

The experimental setup for the time-bin encoded QKD demonstration is shown in Fig. 4.9. The transmitter consists of a 1550 nm continuous-wave laser (Wavelength Reference, Clarity-NLL-1550-HP) that is intensity modulated by electro-optic intensity modulators (IM) to create $\sim$ 66 ps-width optical wavepackets. An electro-optic phase modulator (PM) controls the phase of each wavepacket. A system clock rate of 2.5 GHz gives a bin width of 400 ps, much larger than the width of the optical pulse and the detection jitter of the receiver system (detectors and electronics). A field-programmable gate array (FPGA) (Altera Stratix V 5SGXEA7N2F40C2) drive the IM and PM to create the necessary patterns for each state in the temporal and phase basis. A second IM is used to control the intensity of decoy-states which are used to bound the mulit-photon wavepackets that are present from our coherent light source (Lo et al., 2005). The wavepackets are attenuated to the single photon level and sent through the quantum channel to Bob's receiver, comprised of high-efficiency SNSPDs and the GaAs MMIC amplifier read-out scheme discuss

in this chapter. Bob's basis choice is done passively with a 1×2 beamsplitter and routed to one of four temporal-basis detectors (Dt) or to the interferometer tree for a phase-basis measurement. The time-basis measurement scheme has a 1×4 splitter to limit detector saturation and enable a higher detection rate. Detection signals are recorded by a time-tagger (Agilent, Acqiris U1051A) with a 50 ps resolution. The time delay and phase settings for the interferometer tree are discussed in Chapter 2.

The results of the QKD demonstration are shown in Fig. 4.10. We have achieved record-high secret key rates (SKR) at each channel loss with a maximum rate of 26.2 Mbits/s. We also maintain low BER under $\sim$ 5% at each channel loss. The SKR agrees well with the security analysis (Tomamichel et al., 2012) of our protocol which includes information reconciliation, privacy amplification, finite key effects, reduced detection efficiency at high count-rates, and state-preparation and measurement (SPAM) errors.

4.6 Conclusion

In this chapter I have described the development of a low-noise, low-power cryogenic read-out circuit to enhance the performance of SNSPDs. Critical detector characteristics such as maximum count rate and timing resolution are heavily influenced by the electrical read-out circuit. I have developed a simple, scalable solution that has demonstrated rates exceeding 20 Mcps and timing-jitter as low as 35 ps. The scalable cryogenic read-out circuit coupled with high-efficiency SNSPDs enabled a record-setting secret key rate of 26.2 Mbit/s to be achieved in a proof-of-principle time-phase QKD protocol.

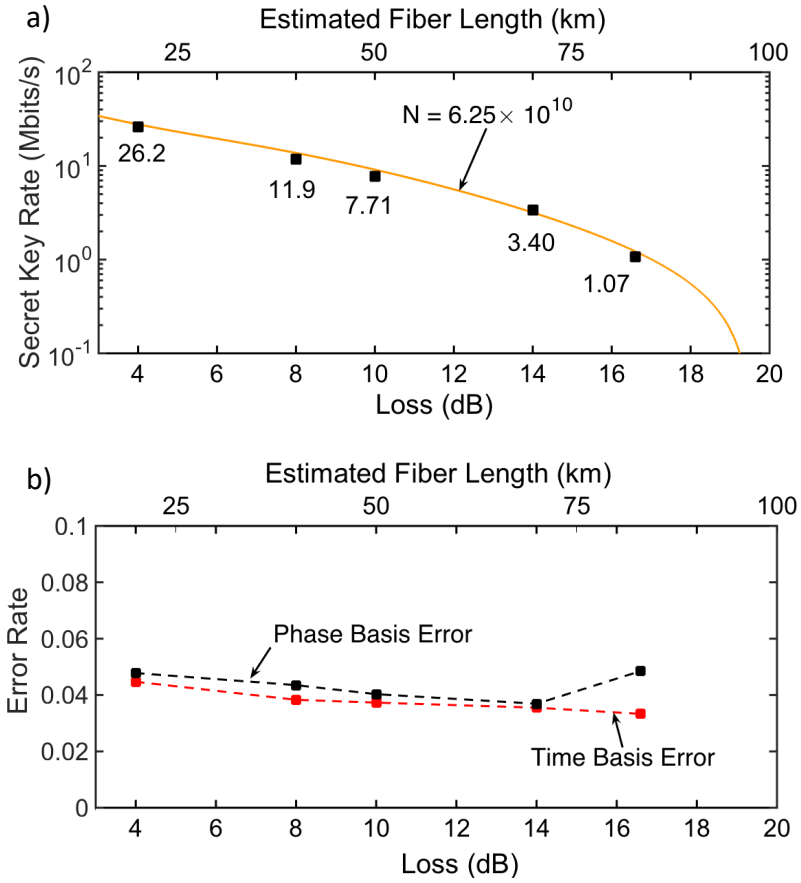

FIGURE 4.10: Results of the time-bin encoded QKD demonstration with $d = 4$ (Islam et al., 2017a). (a) Secret key rate (SKR) as a function of channel loss or an equivalent fiber length assuming a propagation loss of 0.2 dB/km. Black squares are experimentally measured data points and the orange curve is the theoretically predicted SKR from the security analysis which takes in to account experimental parameters such as finite key effects, decreased detection efficiency at high count-rates, and state-preparation and measurement (SPAM) errors. N=6.25×10^{10} is the number of transmitted signals. The recorded data agrees well with the predicted curve. (b) BER for each data point in the time-basis and frequency-basis.

5

Multi-Photon Detection

In the previous two chapters I have discussed the utility of SNSPDs and the advantages they offer in quantum communication protocols. Namely, SNSPDs outperform other detectors in detection efficiency, dark count rate, maximum count rate, and timing resolution. Additionally, Chapter 4 detailed the optimization of the read-out circuit to enhance the detector performance. Despite the high performance of SNSPDs in most metrics, they have historically lacked the ability to resolve the number of incident photons.

Typically, SNSPDs operate in Geiger mode, where a threshold is applied to the electrical signal generated by the read-out circuit indicating the detection of at least one photon. However, there are many experiments where it is highly desirable or even necessary to use detectors that resolve the photon number n. Number resolving power is advantageous for the development and characterization of on-demand single-photon sources such as quantum dots (Intallura et al., 2007) or spontaneous parametric down conversion (SPDC) sources (Kaneda et al., 2015; Guilbert and Gauthier, 2015) that have been useful for quantum information experiments. For example, entangled photon pairs can be generated by driving a SPDC crystal with a

strong pump laser. Photons are born at the same time and the detection of one photon heralds the presence of the other. To increase the speed and efficiency of photon production the pump laser power can be increased, but at the expense of an increased generation rate of degenerate photon pairs. Using a heralding detector with PNR capabilities, the deleterious multi-photon events can be selected against and allow only single-photon pairs to contribute to experiments. Additionally, photon-number resolving power could enhance quantum communication experiments by increasing the channel capacity or providing an efficient way to ensure the security of the channel (Cattaneo et al., 2018).

To address this issue, several groups have devised ways to use Geiger-mode SNSPDs to emulate photon-number-resolving detectors, including: spreading the wavepacket across a detector array (Divochiy et al., 2008; Dauler et al., 2009; Moshkova et al., 2019); temporal multiplexing (Kruse et al., 2017); and operating the detector with a low bias so that only multi-photon events are recorded (Bitauld et al., 2010). While these approaches are adequate for some applications, they often compromise other outstanding performance metrics of the SNSPD or lead to complex systems. Other devices, including visible-light photon counters (Kim et al., 1999) or transition-edge sensors (Miller et al., 2003), have degraded metrics, such as higher dark count rates or slower response time, among others.

In this chapter I present multi-photon detection using a conventional single-pixel SNSPD, where photon-number resolution arises from a time- and photon-number-dependent resistance R_{hs} of the nanowire during an optical wavepacket detection event. The different resistances give rise to different rise times of the generated electrical signal, which can be measured using a low-noise read-out circuit. The observed signals are consistent with an electro-thermal model of the device, which accounts for the basic properties of the superconducting nanowire coupled to the read-out circuit and the Poisson statistics of the weak coherent source illuminating

the detector.

5.1 Detection Dynamics of SNSPDs

The lumped-element model of the detector consists of an inductor L_k arising from the kinetic motion of the superconducting Cooper pairs, and a switch in parallel with the total nanowire resistance nR_{hs}. In the dark, the switch is closed and the current flows through the zero-resistance path of the detector. When one or more photons are absorbed in the film, as illustrated in the inset of Fig. 5.1, Cooper pairs break, and the temperature of the wire segments go above the critical temperature and hence into the normal state, creating n hot-spots. Hot-spot formation is modeled as the opening of the switch. Joule heating of the normal segments and thermal diffusion cause the hot-spots to grow, eventually stagnating due to the combined effects of heating, diffusion, and cooling to the substrate. Typically, the stagnated value of $nR_{hs} \gg R_L$ and hence most of the current is shunted to the read-out circuit. After a period of $\sim$ 300 ps, cooling to the substrate dominates, the hot-spot collapses, and the wire returns to the superconducting state, effectively closing the switch.

To predict quantitatively photon-number-resolving detection, we generalize a model for the detector and read-out circuit known as the electro-thermal model (Kerman et al., 2009). Here, the dynamics of R_{hs} and the current flowing through the detector are described by a set of coupled nonlinear differential equations, given by,

$$L_k \frac{dI_{det}}{dt} = -nR_{hs}I_{det} + (I_{bias} - I_{det})\, R_L, \tag{5.1}$$

$$\frac{dR_{hs}}{dt} = \frac{2R_{max}}{l} v(I_{det}), \quad 0 \leqslant R_{hs} \leqslant R_{max} \tag{5.2}$$

where R_{max} is the total resistance when the entire length l of the wire is in a resistive state. The parameter $v(I_{det})$ is the phase front velocity of an individual hotspot.

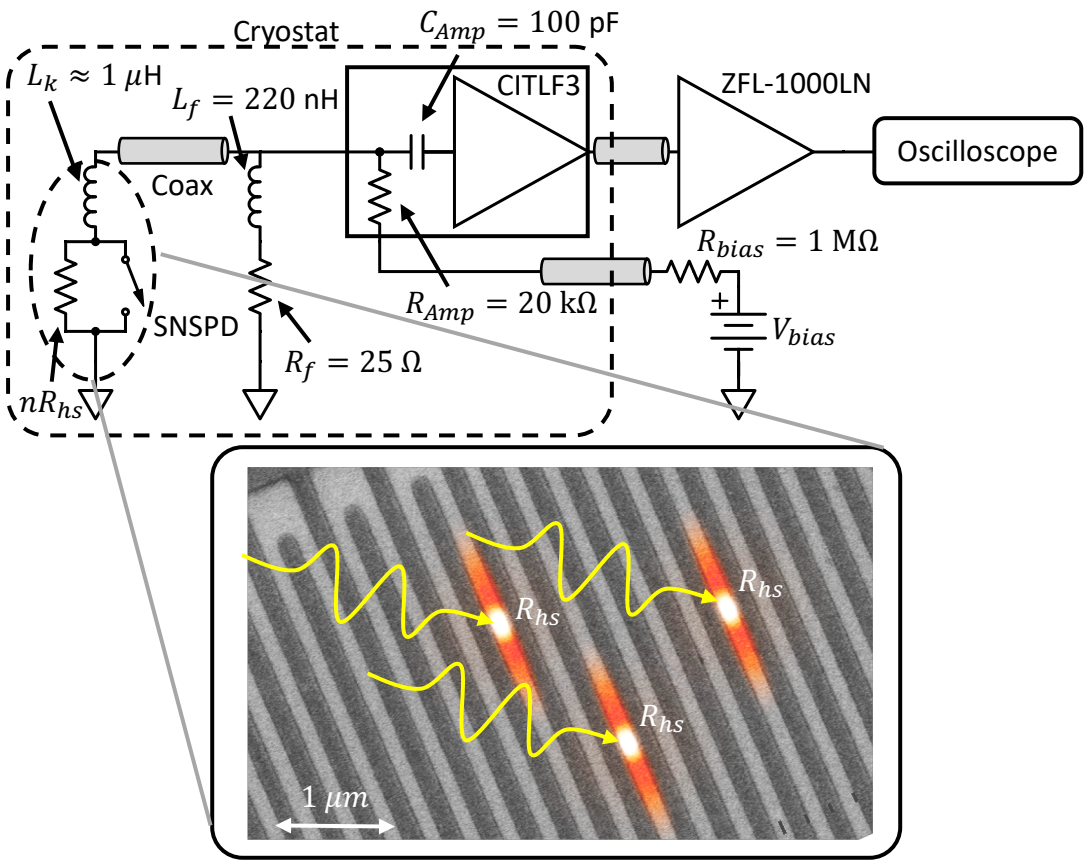

FIGURE 5.1: Detection schematic for collecting undifferentiated detection waveforms generated at the SNSPD (Nicolich et al., 2018). The resistor nR_{hs} is total resistance of the detector where the value of R_{hs} is a function of the total number of photons absorbed. The circuit schematic as depicted here is used to collect raw, undifferentiated waveforms. Not shown is an optional analog differentiation filter inserted before the oscilloscope. (Inset) Multiple photon detection events depicted in a scanning electron micrograph image of an SNSPD where each hot spot has a resistance R_{hs}.

Equation 5.1 is derived from Kirchhoff's law and describes the distribution of current in the circuit, and Eq. 5.2 describes the time evolution of a single hotspot. In the analysis we assume that the n hot spots do not overlap spatially and hence each is governed by an identical differential equation. The total resistance of the nanowire due to the presence of n hot spots is given by nR_{hs}.

An analysis of the model reveals that the stagnated value of R_{hs} depends on n

due to its coupling to the current equation. Furthermore, we find that the resulting rise time of the voltage generated at R_L scales approximately as $1/\sqrt{n}$ (Nicolich et al., 2018). Additionally, a complete analysis by Nicolich et al. (2018) reveals a universal model for the rising edge during the turn-on of the detector resulting from photon absorption. This model predicts the rise-time of the detection waveform as a function of nanowire length l, bias current I_{bias}, and number of absorbed photons n. The details of the universal model are outside the scope of this thesis.

5.2 Experimental Results

To test our predictions, we generate short optical wavepackets by intensity-modulating a 1550-nm-wavelength continuous-wave laser, attenuating to result in a mean detected photon number μ, and couple the wavepackets into a single-mode fiber that delivers the light to the detector. The modulators are driven by signals generated from an FPGA which allows course control of the repetition rate of the pulse train and width of the wavepacket (limited by the bandwidth of the modulators). A slow repetition rate of $\sim 1\,\mathrm{MHz}$ is desired in order to limit the negative effects caused by the detector recovery time. However, a repetition rate that is too slow will result in an artificial increase in the $n = 1$ counts because of the very small duty cycle and finite extinction ratio of the modulation. The temporal wavepacket width ($\leqslant$100 ps) is shorter than the expected stagnation time of the hot spot, which is required for our read-out scheme to detect multi-photon events. The source setup is shown schematically in Fig. 5.2.

The detector used in this study consists of a single meandering wire which is made of a proprietary amorphous superconducting material from Quantum Opus. It is current biased (I_{bias}) and connected to a DC-coupled, high-bandwidth, cryogenic read-out circuit (CITLF3, Cosmic Microwave Technologies) with an effective load resistance $R_L \simeq 50\ \Omega$. A DC-coupling is provided by an L-R filter between the

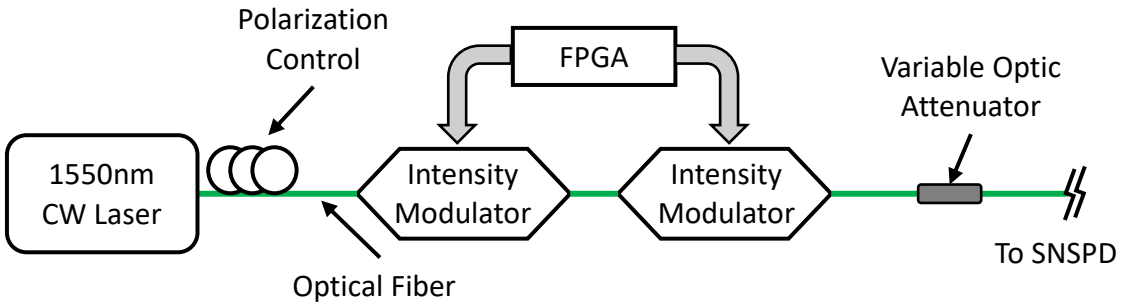

FIGURE 5.2: Experimental setup to create short-duration, multi-photon wavepackets (Nicolich et al., 2018). An FPGA drives electro-optic intensity modulators creating short optical wavepackets. Two modulators are used to increase the extinction ratio of the on/off modulation.

detection and the coupling capacitor of the amplifier. This filter provides a DC path-to-ground while preserving the bandwidth of the amplifier (Cahall et al., 2018). High-bandwidth amplifiers are important for resolving n because this information is encoded in the rise time of the detection waveform.

Raw waveforms collected at the output of the room temperature amplifier, shown in Fig. 5.3b, display clear changes in the slope of the rising-edge. However, in practice it is challenging to discriminate rise-time changes of individual pulses in real-time measurements. Therefore, we convert the rise time to an amplitude using an analog inductor-resistor differentiating circuit shown in Fig. 5.3c. It is clear that the difference between the maximum height of the differentiated waveforms decreases as the value of n increases. This effect is mostly due to the $\sqrt{n}$ dependence of the hot-spot resistance, with a first order correction given by bandwidth limiting effects from the amplifiers.

To provide further evidence of multi-photon detection we use the histogram function of the oscilloscope to collect the probability distribution for the maximum value of the slope of the signal after the differentiating circuit, arising from photon detection events. Figure 5.4 shows the normalized peak-height probability distributions of

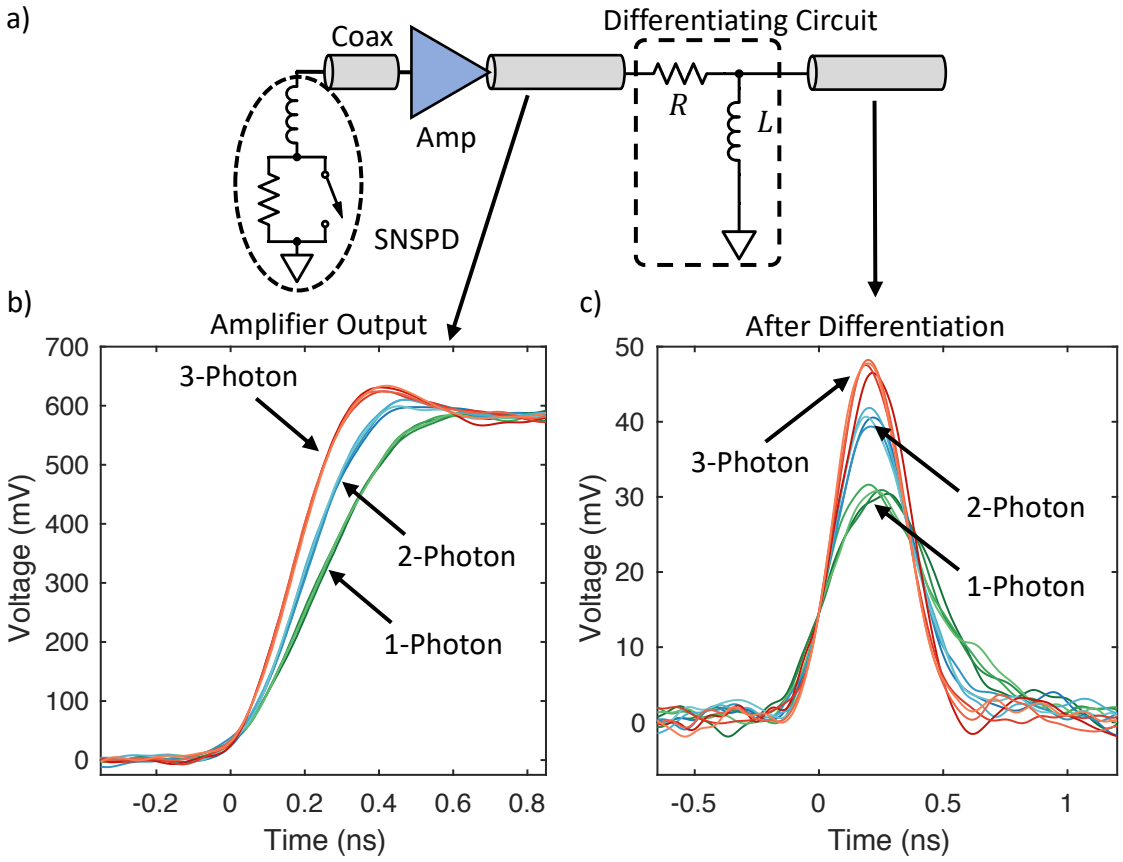

FIGURE 5.3: Photon detection waveforms for $n = 1, 2$, and 3 photons recorded with an 8 GHz analog bandwidth oscilloscope (Agilent Infiniium DSO80804B). (a) Simplified schematic of the two read-out schemes to measure multi-photon detection events. (b) The rising edge of single-shot waveforms collected after the output of the room temperature amplifier. (c) Single-shot waveforms collected after an analog inductor-resistor differentiating circuit.

the differentiated photon detection waveforms for three different values of μ. For low μ values, we clearly observe a primary peak at $\sim$30 mV and a second peak at $\sim$41 mV. At higher μ values, the first two peaks remain at essentially the same value and the height of the second peak grows relative to the first. Furthermore, additional features appear at higher voltages, serving as preliminary evidence for 3- and 4-photon detection events. As an initial analysis, we fit each distribution with two, three, or four Gaussian functions (dependent upon the value of μ), where the center and width

of each Gaussian is a free parameter, but the integral under each curve is constrained by assuming that the photon number distribution follows Poisson statistics.

Previous measurements of this type show good agreement between the collected data and the expected statistics (Cahall et al., 2017). The data presented in Fig. 5.4 show a mismatch between the collected counts and the counts that were expected. This mismatch could be due to several factors. Though careful steps were taken to ensure to an accurate calibration, there could be an unaccounted for error in the calibration which could skew the magnitude of counts expected. A more likely explanation for the mismatch could be due to the finite width of the optical pulse ($\sim 100\,\mathrm{ps}$ in the data shown in Fig. 5.4). An optical pulse with a significantly large width in time compared to the rise-time of the electrical waveform could affect the absorption of photons at $n > 1$ values and becomes worse as n becomes larger. In particular, consider the detector absorbs one photon and starts the process of hot-spot formation. A second (or third, fourth, etc.) photon impinging on the detector at some later time could be sampling the detector in a different state (due to its reaction to the first photon), and therefore could be absorbed with a reduced efficiency or not at all dependent upon the time delay.

The width of each photon-number peak, which dictates the resolving power of the detected photon number, is largely determined by the variation of R_{hs} arising from the non-uniformity of the wire, reduced signal-to-noise ratio in the read-out circuit, and the finite width of our optical pulse. The results of the histogram indicate that high fidelity discrimination between $n = 1$ and $n > 1$ detected photons is possible. The bit-error-rate for $n = 1$ and $n > 1$ discrimination, calculated by computing the area under the $n = 1$ and $n = 2$ curves where they overlap and dividing by the total area of the $n = 1$ curve, is 4.2×10^{-4}. A low BER on the order of 10^{-4} enables discrimination of photon numbers greater than $n = 1$ with $> 99.9\,\%$ accuracy.

Better resolving power, especially at high values of n, could be possible in the

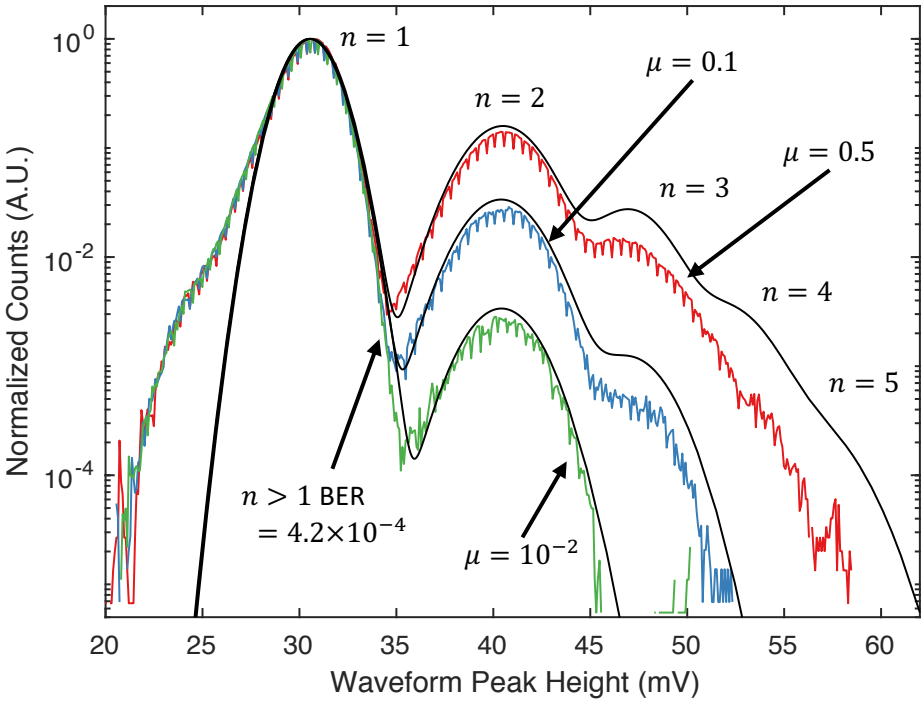

FIGURE 5.4: Histograms of the peak height of differentiated detection waveforms. Each data set is fit with a sum of Gaussian functions (black), where the integral of each peak is constrained to follow the expected Poisson statistics for $\mu = 10^{-2}$ (green), $\mu = 0.1$ (blue), and $\mu = 0.5$ (red).

future by utilizing several strategies. A photon source consisting of a mode-locked laser would be able to create much shorter optical pulse widths compared to the modulator setup that we have used. A shorter duration optical pulse would allow each photon contained in the wavepacket to sample the detector in roughly the same state of operation, contrasted with photons that are distributed in time where later arriving photons might sample the detector once a detection even has already begun to take place. Future measurements with a short optical wavepacket would help give a better understanding of the contributions to the width of the differentiated distributions that are dictated by detector design or read-out noise. The design of the nanowire can be optimized to enhance the photon-number resolution with devices designed having a more uniform R_{hs} or devices able to operate with higher

I_{bias} for a larger signal. Finally, read-out circuits schemes with lower noise and wider bandwidth would improve resolution. More advanced read-out schemes that directly probe the total resistance of the device nR_{hs} can also be devised.

A feature in Fig. 5.4 that must be addressed is the distribution on the left of the $n = 1$ peak that is caused by slower detection waveforms. Preliminary evidence indicates that the slower waveforms causing this distribution are due to detection events caused by background light. Here I make the distinction between background counts and dark counts. Dark counts are detection signals that are not created by photon absorption, but rather a false detection event due to a misfire in the detector. The dark count rate in SNSPDs is practically zero. Background counts are detection signals created by stray photons that get absorbed by the detector. Historically, for these detectors the two terms are used interchangeably.

We estimate that the distribution on the left side of the $n = 1$ peak is due to background counts or dark counts because the height and width of this distribution does not change with the photon number setting. However, the relative height of the left-side counts compared to the $n = 1$ counts changes as a function of detector bias current. The change in the relative number of counts as a function of bias current supports the notion that the counts in the unknown distribution are due to background or dark counts when looking at the comparison of the signal count rate and dark count rate in Fig. 5.5a. The signal count rate is recorded with the laser turned on and the dark count rate is recorded with the laser turned off where detection events with the laser off are due to background/dark counts.

Additionally, ten-thousand raw waveforms are collected at a detector bias current of 12.8 μA ($0.95I_{sw}$) with the laser turned 'on' and 'off.' The waveforms are differentiated numerically and the peak height of the differentiated waveform is recorded. A histogram of peak heights from the differentiated waveforms for laser 'on' (with mean photon number per pulse $\mu > 0.1$) and background counts are shown in Fig. 5.5b.

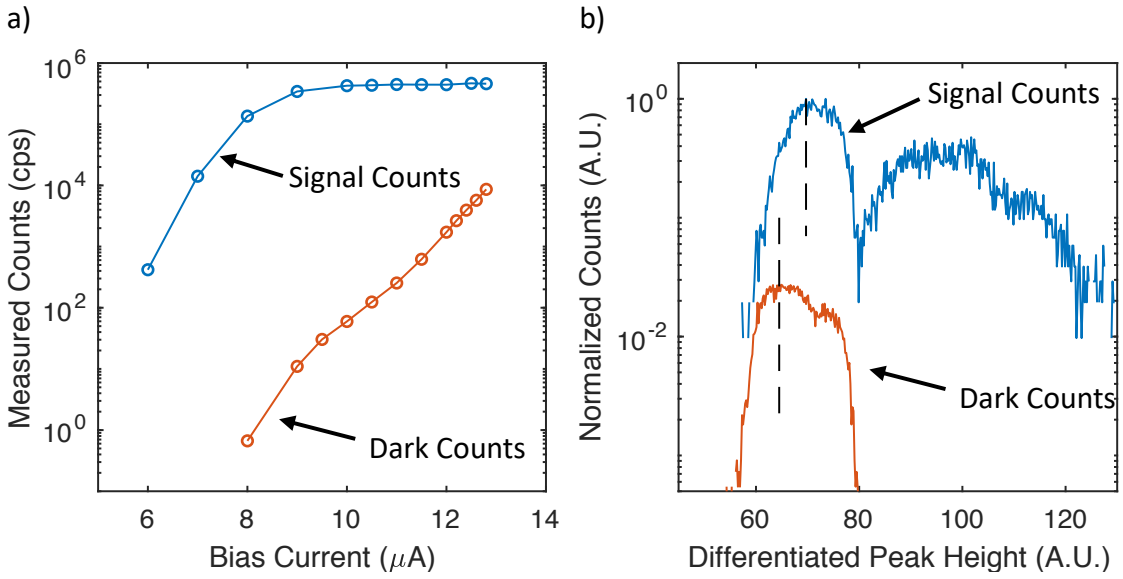

FIGURE 5.5: The effect of dark counts on the distribution of differentiated waveform peak heights. (a) Count rate comparison between the count rate collected when the modulated laser source is switched 'on' and when the source is switched 'off.' (b) Differentiated peak height distribution for a mean photon number $\mu > 0.1$ and detector bias current of 12.8 μA ($0.95I_{sw}$). The distribution is produced by differentiating raw waveforms numerically and creating a histogram of maximum differentiated values. Dotted lines indicate the maximum of the largest distribution for signal and background counts.

The resolution of the histogram in Fig. 5.5b is not as good as the histogram in Fig. 5.4 possibly due to the collection method or the factor of 10^3 fewer counts. However, the asymmetry of the $n = 1$ distribution is still noticeable with a skew toward smaller differentiated peak values. The differentiated peak height histogram of the dark counts clearly shows a large number of waveforms that skew to the left of the center of the signal distribution, indicated by the dotted lines in the figure showing the maximum counts for each curve.

The reason for the change in the waveform rise-time due to dark counts/background counts, if this is indeed the explanation for this distribution, is not completely understood. We hypothesize that the change could be due to some energy dependence of the hotspot due to very long-wave radiation, or intrinsic dark counts within the

device that could operate at slightly different time-scales. However, the universal model for the SNSPD turn-on by Nicolich et al. (2018) does not account for any dependence upon the energy of the detected photon or a dark count mechanism.

5.3 Conclusion

In this chapter I describe a new mode of operation for conventional single-pixel SNSPDs. Typically, SNSPDs lack photon-number resolving capabilities though many groups have devised was to circumvent this shortcoming by using various multiplexing schemes. The work I present here demonstrates the ability for conventional SNSPDs to resolve multiple detected photons without applying advanced multiplexing schemes such as large detector arrays. We experimentally demonstrate photon number detection up to 4-photons where the photon-number is encoded in the rise-time of the electrical waveform generated by the detector. Additionally, our experiment agrees well with the predictions of a universal model for turn-on dynamics of SNSPDs. Finally, our multi-photon detection systems demonstrates high-resolution between $n = 1$ and $n > 1$ photons with a BER of 4.2×10^{-4}.

Future experiments include the development of future detector designs that enhance the resolving power for multi-photon events. The resolution can possibly be enhanced by an optimized detector design and high-bandwidth, lower-noise read-out circuits. Additionally, further investigation must be done to characterize the role that background/dark counts play in the profile of the detection waveform, which may open up new physics in the study of detector and thin film superconducting dynamics.

6

Free-Space Communication

The time-phase QKD protocol discussed in Chapter 2 is well suited for a free-space implementation since temporal states (with bin widths on the order of a few hundred pico-seconds, such as the ones discussed for our system) are robust against errors caused by dispersion from the atmosphere (Kral et al., 2005). However, a careful analysis is necessary when designing systems for free-space optical communication. A complete system design for a time-phase QKD protocol must include: wavelength choice, transmitting and collection optics, spectral filtering, and measurement infrastructure including time-delay interferometers and single-photon detectors. The most important consequence of establishing a free-space communications link is the resulting spatial mode of the beam at the receiver due to atmospheric turbulence. Unlike the single-mode, fiber-based demonstration discussed in Chapter 4, a free-space communication will inherently be a multi-mode system. Therefore, the receiver infrastructure, and most importantly the time-delay interferometer needed to make phase-basis measurements, must also support many spatial modes.

Several groups have demonstrated classical and quantum interference with multi-mode time-delay interferometers that employ different approaches to enable maxi-

mum visibility. High order spatial modes have differing k-vectors and therefore will have different propagation lengths through the system, potentially degrading the total interference of the beam. A technique to reduce the mode-dependent path length uses a $4\text{-}f\text{-}$imaging system in each arm to relay the mode during propagation and therefore remove the k-vector dependence (Agne et al., 2016; Zeitler et al., 2016), demonstrating fringe visibility as high as 93%.

Another promising design for multi-mode interference is a field-widened Michelson-type interferometer without relay optics. One such design has been demonstrated to have a high fringe visibility (90% reported) and high entanglement visibility (Jin et al., 2018). In this chapter I discuss the design, construction, and characterization of a multi-mode time-delay interferometer utilizing a field-widened design without relay optics. Also, I address the characteristics of the communication link, including the transmitter telescope, receiver telescope, free-space propagation length, and atmospheric turbulence which influence the design and performance of the interferometer.

6.1 Atmospheric Effects

Free-space optical communication links are strongly affected by atmospheric conditions such as turbulence, molecular absorptions lines, and scattering due to particulates (Pollock et al., 1993). Molecules and particles cause absorption or scattering of photons out of the beam which results in increased channel loss. Turbulence distorts the spatial profile of the transmitted beam resulting in a multi-mode field at the receiver. Despite the high degree of difficulty of free-space experiments, several groups have recently demonstrated free-space quantum communication protocols including terrestrial links (Bourgoin et al., 2015; Ursin et al., 2007) and ground-satellite links (Ren et al., 2017; Liao et al., 2017).

6.1.1 Scattering and Absorption

The channel loss due to absorption and scattering is minimized with a proper operating wavelength choice. Typically, light with shorter wavelengths such as those in the visible have larger attenuation due to Rayleigh and Mie scattering, but longer wavelengths overlap more with the 300 K blackbody radiation spectrum which can make background spectral filtering more challenging. Near-infrared (NIR) wavelengths ($\sim 0.75 - 3\,\mu$m) are ideal because they have reduced scattering loss while having minimal overlap with 300 K radiation. Historically, wavelengths $\leqslant 1\,\mu$m were chosen because of the availability of single-photon detectors (due to the large bandgap of silicon, the semiconductor often used for SPADs and other photodiodes, these detectors are invisible to wavelengths $> 1.1\,\mu$m). The recent development of high efficiency SNSPDs in the NIR has allowed a wider range of wavelengths to be explored for communication protocols utilizing single photons.

High resolution atmospheric transmission (HiTRAN) simulations are useful in determining the structure of absorption spectra due to molecules in the atmosphere. The most abundant molecules that affect visible and NIR transmission are carbon dioxide and water. Transmittance simulations including Mie scattering and molecular absorption are shown in Fig. 6.1. A 70 GHz transmission window close to $1.55\,\mu$m is apparent in the high resolution simulation shown in Fig. 6.1b. The transmission window is compatible with operating wavelength of the single-mode system and therefore we can use most of the same transmitter infrastructure as in our single-mode demonstration. Additionally, a 70 GHz window is able to support multiple wavelength (frequency) channels using wavelength division multiplexing (WDM) schemes that are common for communications in the telecommunications band. The atmospheric transmission window can support two channels in a dense WDM scheme with 50 GHz channel spacing, or up to five channels in an ultra-dense WDM scheme with 12.5 GHz

channel spacing.

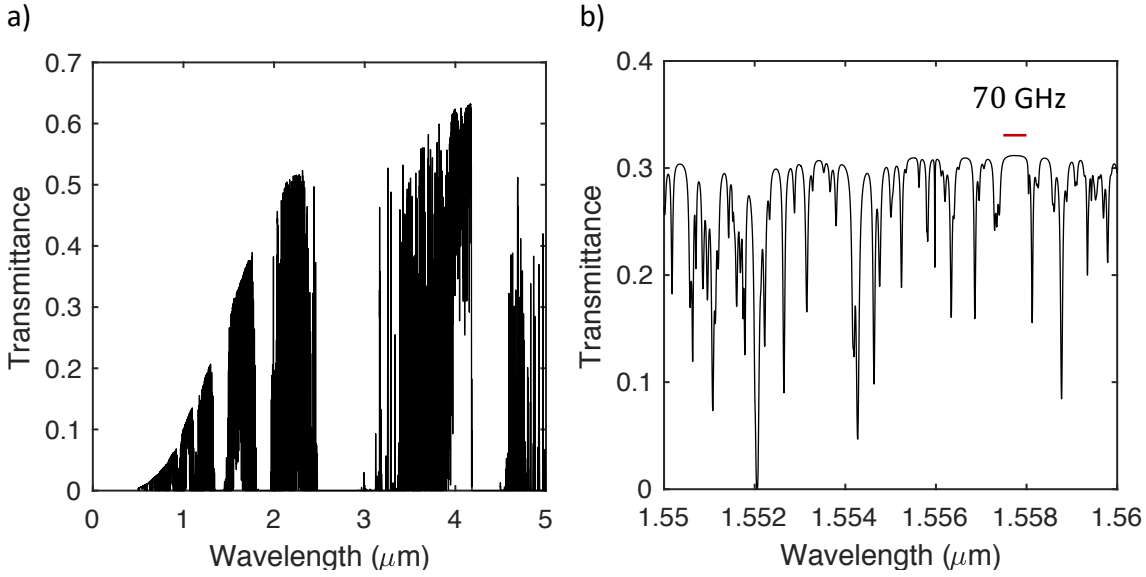

FIGURE 6.1: HiTRAN simulation of a 30 km tropical path including losses from Mie scattering and molecular absorption. (a) Transmittance of $0.5 - 5\,\mu$m wavelength range. (b) Simulation of wavlengths close to $1.55\,\mu$m showing a 70 GHz transmission window.

6.1.2 Turbulence

Turbulence effects are a priority when considering the system design. Spatial variations in temperature and air density result in a refractive index structure that varies across the profile of the beam. Small differences in the refractive index cause refraction, leading to interference and mode-mixing. The strength of turbulence is often described by a single parameter C_n^2, a number that quantifies the refractive index structure in the atmosphere (Tatarski, 1971; Wesely, 1976). A proper characterization of atmospheric turbulence and the effect it has on the optical beam is necessary to design an optimized interferometer.

Propagation of light through turbulent atmosphere is typically approximated in the lab using spatial light modulators (SLM) programmed with a random phase

pattern (Hill et al., 2016). The beam is reflected off the SLM where the spatially random phase is imprinted on the beam, followed by a free-space propagation. The beam is often reflected off the SLM several times before being analyzed. Simulations of turbulent propagation are performed in a similar way. The free-space link is discretized in to alternating sections of vacuum propagation and an interaction with a two-dimensional randomized phase screen (Chesnokov et al., 1995). This method allows turbulence to easily be simulated using computer software such as MATLAB (Schmidt, 2010).

I perform propagation simulations for three turbulence values, four link distances, and three transmitter apertures. Each setting in this array is simulated 20 times to analyze the average behavior such as beam size and receiver loss. Ten phase screens are evenly spaced across the link distance between the source plane and the observation plane. The phase screens and observation plane each have a resolution of 1 mm and a 2 m diameter. The beam size is computed by averaging the intensity from the repeated simulations and calculating the $1/e^2$ radius at each link distance. Then, the size as a function of distance are fitted with a third-order polynomial which is used to compute the beam's divergence angle by calculating the derivative of the fitted function. The beam size and divergence angle are important because of the requirement to conserve etendue. The conservation of etendue implies that the product of the beam size and divergence angle must be conserved or increase, but cannot decrease. Therefore, the etendue of the beam at the receiver will determine the coupling efficiency from the receiver optics to the interferometer.

Beam analysis from the turbulence simulations are shown in Fig. 6.2. My analysis indicates the beam size and divergence angle after free-space propagation are compatible with multi-mode fiber coupling. For example, the geometric loss due to aperture clipping and etendue for a 50 μm core fiber with a numerical aperture (NA) of 0.12 are shown in Fig. 6.2b. A fiber coupled interferometer greatly simplifies the

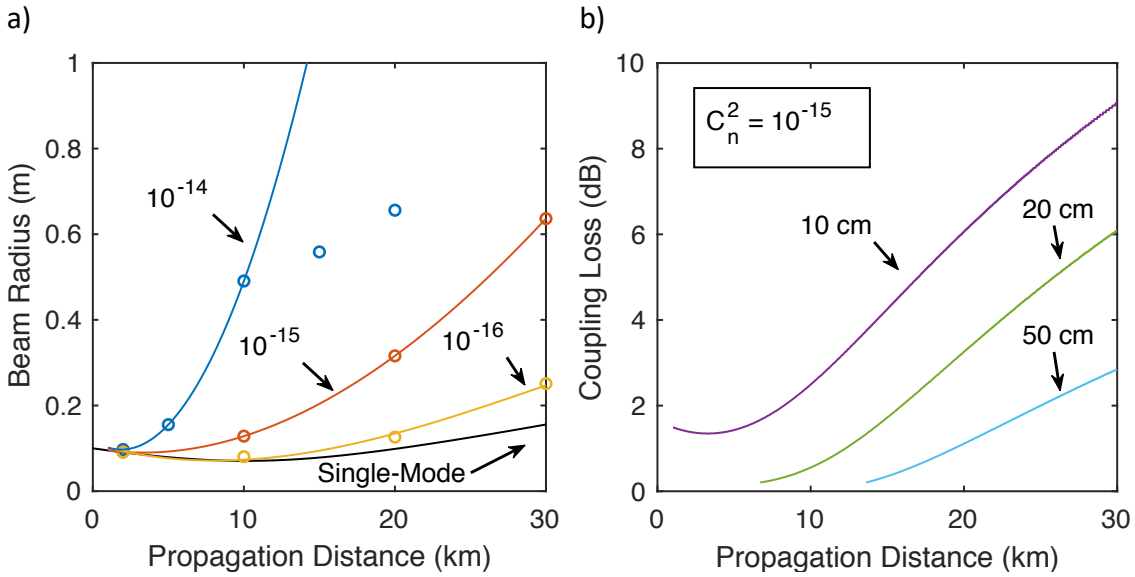

FIGURE 6.2: Results of the turbulent simulation analysis. (a) Beam size (radius) as a function of propagation distance for a 20 cm diameter transmitter and three C_n^2 values. Each data point is the average of 20 simulations and a single mode beam profile is shown in black for comparison. The points in the $C_n^2 = 10^{-14}$ data that stray from the fitted line are simulation artifacts due to clipping by the phase screen aperture. (b) Geometric coupling loss computed for a 20 cm diameter transmitter, $C_n^2 = 10^{-15}$, three different collection aperture diameters ,and a 50 μm core fiber with a 0.12 NA. Loss is computed by aperturing the beam and satisfying conservation of etendue.

receiver design and reduces variations in the characteristics of the input beam, such as beam size, divergence angle, and beam pointing, that is potentially difficult to de-couple from the receiving telescope.

6.2 Multi-Mode Delay Interferometer Design

The multi-mode interferometer design closely follows a Michelson-type that was developed in the 1980's to measure wind speed and temperature in the upper atmosphere (Shepherd et al., 1985; Gault et al., 1985). A simplified interferometer layout is shown in Fig. 6.3.

A ray incident from the left at an angle θ is split at a non-polarizing beamsplitter

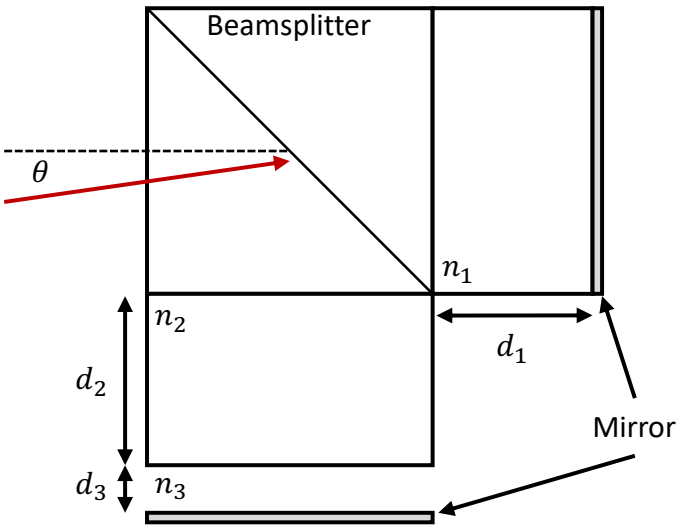

FIGURE 6.3: Simplified schematic of a Michelson-type interferometer. This setup includes a small air gap at the end of the long arm (d_2).

where the beam is directed in to one of two pathways. Relative to each other, one path has a short propagation length and the other has a long propagation length. The short arm is made of material with index n_1 and thickness d_1 and the long arm is made of material with index n_2 and thickness d_2. There is also an air gap of thickness d_3 between the end of the long arm material and the reflector. The two beams are reflected at the end of each arm and recombine at the beamsplitter.

The path length difference Δ as a function of incident angle θ is given by (Shepherd et al., 1985),

$$\Delta = 2[n_3 d_3(1-\sin^2\theta/n_3^2)^{1/2} + n_2 d_2(1-\sin^2\theta/n_2^2)^{1/2} - n_1 d_1(1-\sin^2\theta/n_1^2)^{1/2}]. \tag{6.1}$$

Typically, a Michelson interferometer is designed for the input ray to enter at normal incidence and angular bandwidth is analyzed for small deviations from normal. In the design I present here, the input ray must enter at a finite angle θ_0. A finite

input angle is needed to spatially separate each output beam from the input beam, since access to both outputs are required for the QKD protocol. Unlike the analysis performed in Shepherd et al. (1985) where Eq. 6.1 is expanded about a normal incident angle, I expand Eq. 6.1 about a finite input angle θ_0, and the first three terms are shown in Eq. 6.2.,

$$\begin{aligned}\Delta = 2\left(d_3\beta_3 + d_2\beta_2 - d_1\beta_1\right) - 2\Phi(\sin\theta - \Phi)\left(\frac{d_3}{\beta_3} + \frac{d_2}{\beta_2} - \frac{d_1}{\beta_1}\right) \\ -(\sin\theta - \Phi)^2\left(\frac{n_3^2 d_3}{\beta_3^3} + \frac{n_2^2 d_2}{\beta_2^3} - \frac{n_1^2 d_1}{\beta_1^3}\right)\end{aligned} \tag{6.2}$$

where the input angle $\Phi = \sin\theta_0$ and the effective index of refraction $\beta_i^2 = n_i^2 - \Phi^2$. The goal of my analysis is to satisfy three conditions that are derived from Eq. 6.2. A full derivation of the mathematical results presented can be found in appendix A.

6.2.1 Design Requirements

The interferometer is designed to achieve the following; (1) the optical path-length difference (OPD) be equal to 200 ps (5 GHz free spectral range), (2) satisfy the field-widened condition (discussed more below) for a large angular bandwidth, and (3) the interferometer be thermally compensated. A successful design will feature high visibility (ideally $> 95\%$), long-term temperature stability over a modest temperature range ($\pm 0.2^\circ$ C), and have phase-tuning ability over a complete interference fringe.

The OPD of the central ray is calculated by setting $\sin\theta = \Phi$, leaving only the first term of Eq. 6.2. The path difference Δ is in units of length, and therefore must be converted to a time delay Δ_t by dividing by the vacuum speed of light c, shown in Eq. 6.3.

$$\Delta_t/2 = (d_3\beta_3 + d_2\beta_2 - d_1\beta_1)/c \tag{6.3}$$

A wide angular bandwidth is necessary for a multi-mode interferometer design because a multi-mode beam has a range of k-vectors and each will take a slightly different path through the interferometer. To achieve high visibility the change in OPD as a function of input angle must be minimized. Field-widening is achieved by proper material and geometry choices that make the second term in Eq. 6.2 vanish. The field-widening conditions is

$$\frac{d_3}{\beta_3} + \frac{d_2}{\beta_2} - \frac{d_1}{\beta_1} = 0. \tag{6.4}$$

The result of satisfying Eq. 6.4 is that the OPD in Eq. 6.2 becomes first-order insensitive to deviations from the central input angle.

Lastly, thermal compensation provides long-term stability in an imperfectly controlled environment. Temperature fluctuations cause OPD changes due to expansion and contractions of the physical length of each material, as well as temperature dependent changes in the index of refraction. A proper material and length choice in each arm make the OPD shift in each arm equal and therefore offsetting. The thermal drift is characterized by taking the partial derivative of Eq. 6.2 with respect to temperature T, as

$$\frac{\partial \Delta}{\partial T} = 2d_2 \left[\beta_2 \alpha_2 + \frac{n_2}{\beta_2} \left(\frac{\partial n_2}{\partial T} \right) \right] - 2d_1 \left[\beta_1 \alpha_1 + \frac{n_1}{\beta_1} \left(\frac{\partial n_1}{\partial T} \right) \right]. \tag{6.5}$$

where $\alpha_i = (1/d_i)(\partial d_i/\partial T)$ is the coefficient of thermal expansion (CTE). This analysis assumes that the index and length change of the air gap with temperature is negligible and therefore those terms vanish when taking the derivative (more details can be found in Appendix A). The interferometer is made a-thermal by setting $\partial \Delta/\partial T = 0$, putting a constraint on the path lengths d_1 and d_2, given by

$$\left[\beta_1\alpha_1 + \frac{n_1}{\beta_1}\left(\frac{dn_1}{dT}\right)\right] d_1 = \left[\beta_2\alpha_2 + \frac{n_2}{\beta_2}\left(\frac{dn_2}{dT}\right)\right] d_2. \tag{6.6}$$

6.3 Performance Simulation

I conduct a survey of optical glass with the goal of identifying two glass types to construct the interferometer. The basic guidelines I use for making the glass choices are availability, a large difference in index of refraction between the two materials, and small relative changes in refractive index and length with temperature. A large difference in the index of refraction will enable smaller physical lengths to satisfy a given time-delay.

The finalized design uses N-BK10 for the short arm and N-SF66 for the long arm, both produced by Schott AG. N-BK10 has a CTE of $\alpha_1 = 5.8 \times 10^{-6}\,\mathrm{K}^{-1}$, index of refraction of $n_1 = 1.4823$, and $\partial n_1/\partial T = 1.4154 \times 10^{-6}\,\mathrm{K}^{-1}$. N-SF66 has a CTE of $\alpha_1 = 5.9 \times 10^{-6}\,\mathrm{K}^{-1}$, index of refraction of $n_2 = 1.8660$, and $\partial n_1/\partial T = -1.5575 \times 10^{-6}\,\mathrm{K}^{-1}$. The index and change in index for each material are calculated at $\lambda = 1550\,\mathrm{nm}$ using the Sellmeier equation and its derivative with respect to temperature.

The lengths d_1 and d_2 are optimized for an input angle $\theta_0 = 3^\circ$ and satisfy the OPD, field-widened, and a-thermal conditions. However, when satisfying these three conditions simultaneously the physical dimensions of the interferometer are large ($> 50\,\mathrm{mm}$). The consequence of large glass pathways are; (1) large glass path lengths increase the amount of the thermal mass to be stabilized and can increase the settling time for phase tuning, (2) as the path length increases so does the clear aperture required for a beam input at a fixed input angle, and (3) longer path-lengths will be more sensitive to overlap misalignment at the beamsplitter. Misalignment is especially sensitive for multi-mode interference because the spatial frequency of the

mode can easily be on the order of the alignment tolerance, whereas in single-mode interference the mode size is large compared to the alignment tolerance and therefore is less sensitive to misalignment.

The goal of my design is to minimize the physical dimensions of the glass beam paths. Minimizing the glass length will allow for a more robust and manufacturable setup. To meet this goal, I relax the thermal requirements of the design and instead satisfy the a-thermal condition approximately, leaving only the OPD and wide-angle conditions to satisfy exactly. I find a unique solution that satisfies Eq. 6.3 and Eq. 6.4 by eliminating the air gap d_3. The OPD of the central ray and field-widened condition for an interferometer without an air gap d_3 are shown in Eq. 6.7 and Eq. 6.8 respectively. The a-thermal condition remains unchanged when removing the air gap.

$$\Delta_t = 2(d_2\beta_2 - d_1\beta_1)/c. \tag{6.7}$$

$$\frac{d_2}{\beta_2} - \frac{d_1}{\beta_1} = 0. \tag{6.8}$$

The absence of an air gap leaves two equations and two free parameters d_1 and d_2. The path lengths that satisfy Eq. 6.7 and Eq. 6.8 are $d_1 = 34.5\,\text{mm}$ and $d_2 = 43.5\,\text{mm}$. At an input angle of $\theta_0 = 3^\circ$ and a beam diameter $\sim 2\,\text{mm}$ (discussed in more detail below), the clear aperture required is $\sim 10\,\text{mm}$. A clear aperture of this size allows me to decrease the square cross-section of the glass rods to $12.7\,\text{mm} \times 12.7\,\text{mm}$ (as opposed to $25.4\,\text{mm} \times 25.4\,\text{mm}$). Additionally, a $10\,\text{mm}$ clear aperture is $< 80\,\%$ of a $12.7\,\text{mm}$ surface and therefore the surface can easily be polished with standard glass processing capabilities.

The angular bandwidth of the interferometer is characterized by plotting the OPD in Eq. 6.2 for a range of input angles θ around the central ray $\Phi = \sin(3^\circ)$. Recall that satisfying the field-widened constraint given in Eq. 6.8 implies that the

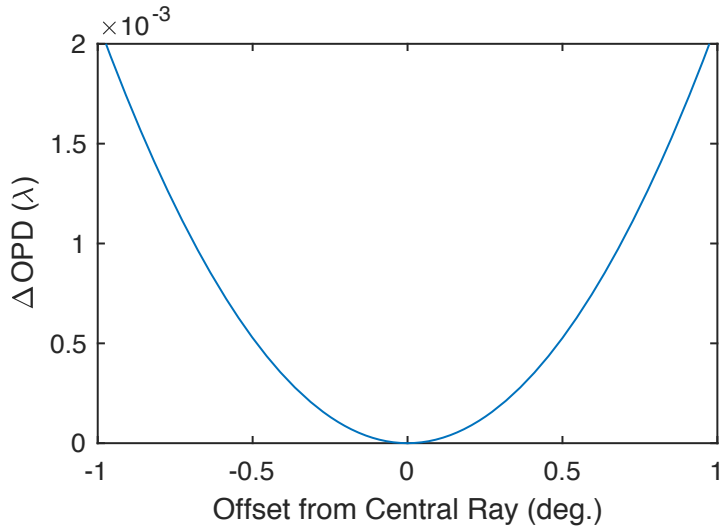

FIGURE 6.4: Angular bandwidth about the central ray of the multi-mode interferometer.

first term in the angular dependence of the OPD proportional to $\sin^2\theta$.

I evaluate the thermal stability of this setup by calculating Eq. 6.5 for small temperature changes ΔT, shown in Fig. 6.5a. The simulation shows that thermal drift $\leqslant \lambda/50$ is achievable for modest temperature fluctuations of $\pm 0.1\,^{\circ}\mathrm{C}$. The phase of the interference is also adjusted with thermal control by adjusting the temperature of one glass path to $\pm 1\,^{\circ}\mathrm{C}$. Temperature control over this range will result in a change in the OPD from $-\lambda/2$ to $\lambda/2$, allowing for a phase tuning range of $\phi = (0, 2\pi)$, shown in Fig. 6.5b. Thermal tuning is preferred over mechanical tuning because mechanical tuning techniques such as piezo-driven mirrors can be expensive, require extra control systems, and have large thermal drifting.

6.3.1 Optical Design Modeling and Simulated Performance

In addition to mathematical analysis I utilize optical modeling software Zemax OpticStudio to aide in the system design. Ray tracing modeling provided by Zemax

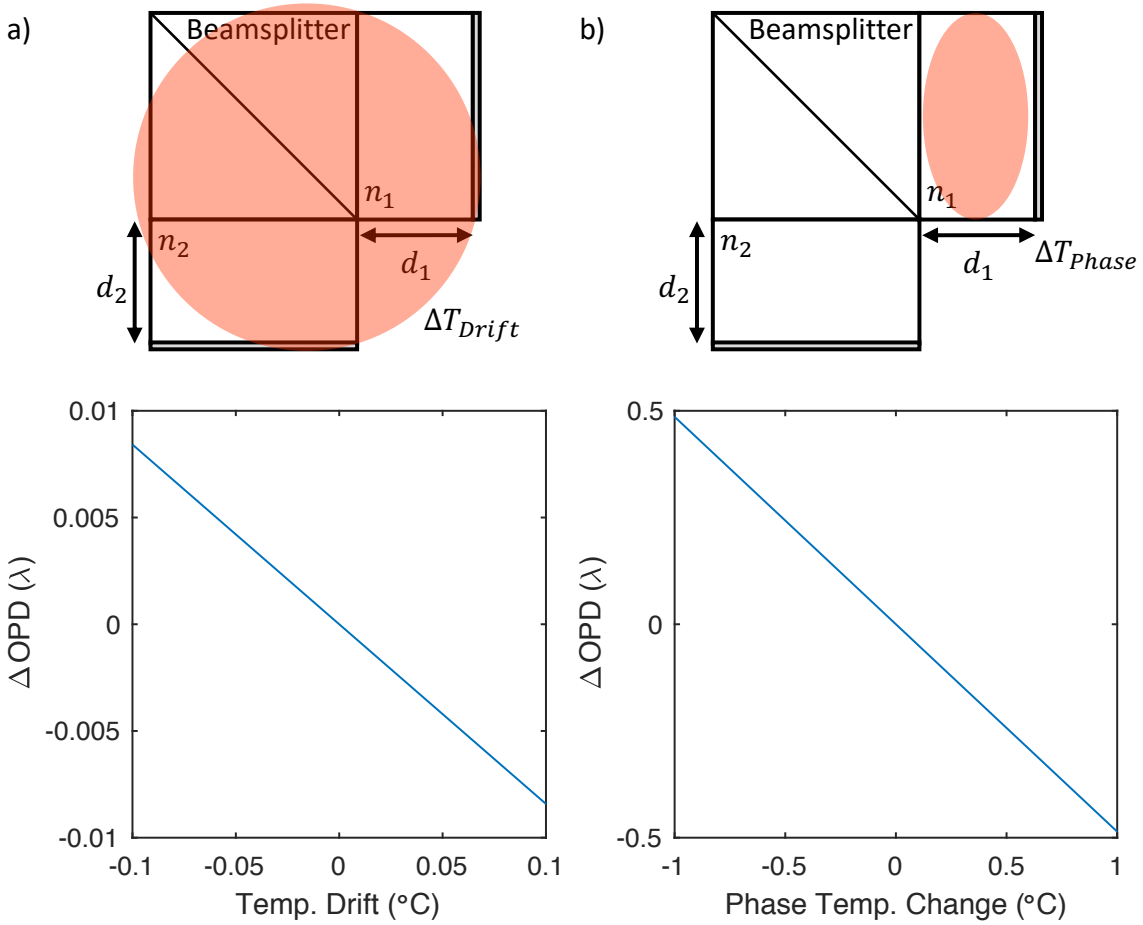

FIGURE 6.5: Simulated thermal performance of the multi-mode interferometer. (a) Thermal stability for small temperature drifts of the complete system. (b) Interference phase tuning via control over the temperature of the short arm d_1.

includes the refraction of the glass at each interferface and is useful in calculating the entry and exit points of the beam for the layout of the input and output optics. In addition, Zemax is used to model beam properties, such as size, and deleterious effects, such as aberrations and clipping, as it propagates through each arm.

A ray tracing diagram for the long arm d_2 is shown in Fig. 6.6a. The beam path in the diagram is comprised of an unfolded mirror image to account for forward and reflected propagation. The input and output fiber coupling lens is a fixed-focus aspheric lens collimator package (f = 8 mm, Thorlabs F240-1550). The output beam

diameter from the 8 mm collimator and a 50 μm core, 0.12 NA fiber is 2 mm. Spot diagrams at the image plane from point sources at the fiber facet indicate that aberrations are minimal and the resulting spot sizes are well within the Airy disc, indicating diffraction-limited performance. The aberrations through the system are minimal since the beam mostly undergoes small angle refraction and remains close to the optical axis of imaging optics. The great imaging performance of the system allows for a high efficiency output coupling in to the fiber, simulated to be $\sim 90\,\%$. Additionally, Fig. 6.6(d-e) show the results of physical beam propagation (single-mode Gaussian waist $w_0 = 1\,\text{mm}$ at output of the collimating lens) through the d_2 arm of the interferometer. The resulting beam profile (viewed in logarithmic scaling) follows a smooth Gaussian function, indicating that there are no clipping effects which would result in distorted wavefront.

6.4 Construction

Construction of the interferometer is carried out with the N-BK10 and N-SF66 glass rods measuring 12.7 mm × 12.7 mm × 34.5 mm and 12.7 mm × 12.7 mm × 43.5 mm respectively, where the long dimension is the optical direction. The end faces are optically polished and coated with an anti-reflective dielectric coating that is optimized for 1550 nm. The glass rods are mounted to a substrate of Kovar nickel alloy. The CTE of Kovar is $\alpha_{\text{Kovar}} = 5.86 \times 10^{-6}\,\text{K}^{-1}$ and is closely matched to the glass in our design. A good match between the glass and substrate, rather than using an ultra-low expansion (ULE) substrate with a much smaller CTE, is advantageous because close match in the CTE between the glass and substrate will minimize the stress on the glass during temperature changes which can cause birefringence and refraction.

A computer-aided design (CAD) model of the complete interferometer system with input and output fiber coupling and beam steering optics is shown in Fig. 6.7.

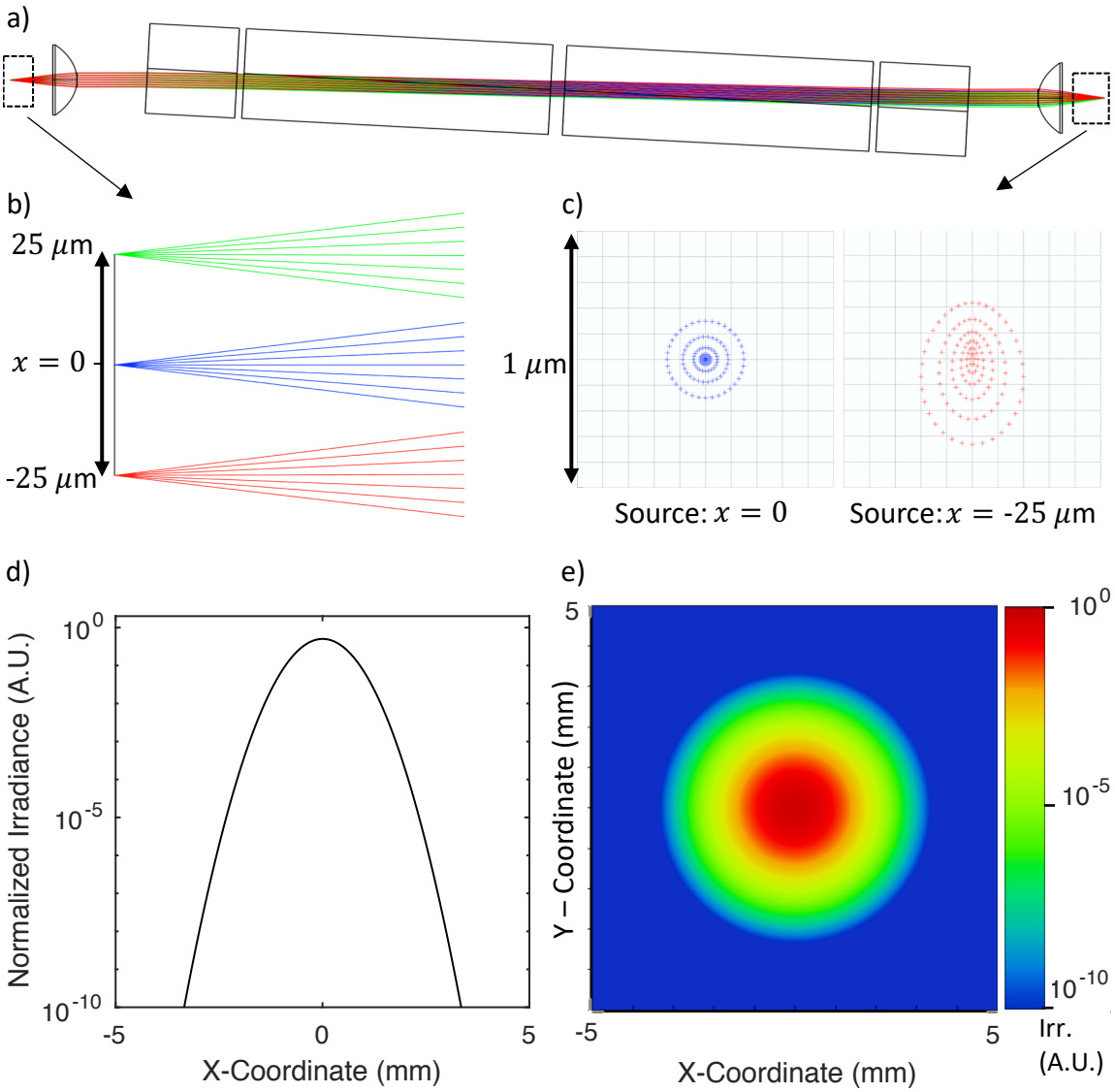

FIGURE 6.6: Zemax simulation results of the long arm beam path. (a) Ray tracing through an unfolded d_2 beam path shown with f = 8 mm aspheric collimating lenses for collimating and fiber coupling. (b) Point sources with 0.12 NA at $x = 0$ and $x = \pm 25\,\mu$m to model the system impulse response from the center and extremes of a 50 μm core fiber. (c) Spot diagrams for the $x = 0$ and $x = -25\,\mu$m point source. For reference, the Airy radius for these spot diagrams is 7.8 μm. (d) The $y = 0$ slice and (e) Spatial irradiance distribution of a single-mode Gaussian beam after propagating through the system to the surface of the collection lens.

The input fiber is collimated with a collimating package (f = 8 mm asphere, discussed above) that is mounted in a custom-machined mount made of stainless steel. Beam

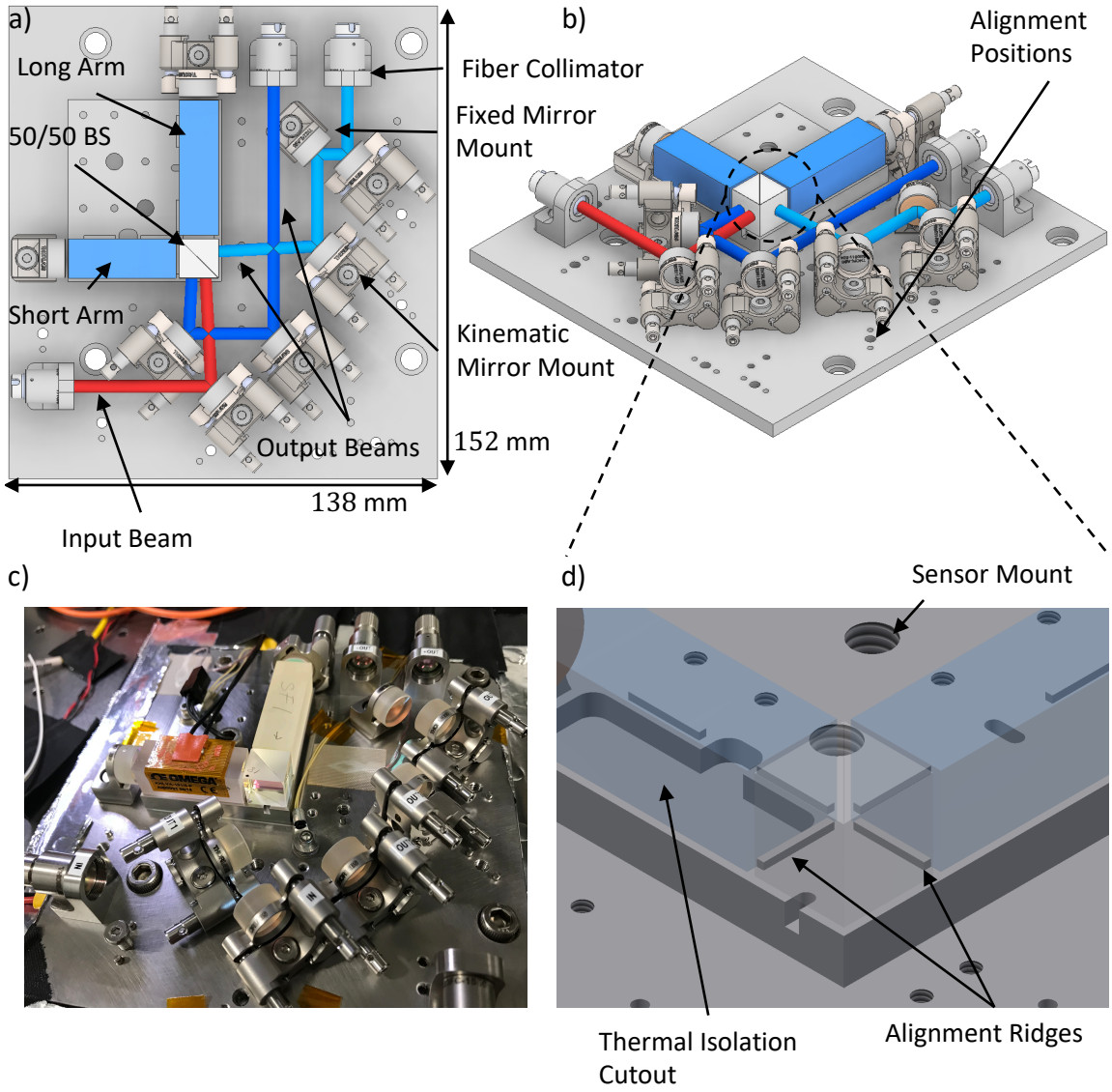

FIGURE 6.7: CAD schematic of the interferometer with input and output beam steering and coupling optics. Overhead CAD view (a) and perspective view (b) of the interferometer layout. (c) Photograph of the assembled interferometer. The heater tape is shown on the short arm glass and several temperature sensors are placed at various positions on the contact plate. (d) Detailed view of the beamsplitter and glass rod alignment features as well as the substrate cutout for thermal isolation of the short arm glass.

steering (for both input and output beams) is achieved by a combination of kinematic (POLARIS-K05C4, Thorlabs) and fixed (POLARIS-C05G, Thorlabs) mirror mounts

using ULE mirror substrates (BB0511-E04, Thorlabs). Optical elements are placed with precision dowel pin alignment holes that are machined in to the Kovar plate via computer numerical control (CNC) milling. Matching dowel holes are in each of the mirror mounts as well as the custom collimator mount. The optical plane is defined by the center of the collimating lenses and the center of the mirrors, both of which are 12.7 mm from the surface of the kovar plate. The non-polarizing beamsplitter (Newport 05BC16NP.11) and glass rods are mounted on a platform in order to bring the center of these pieces up to the optical plane. The beamsplitter and glass rods are aligned on the substrate via 1 mm-height, 1 mm-width raised ridges.

There are two important differences between the schematic and the simulated system discussed earlier. The assembled system has 1 mm gaps between the beamsplitter and glass rods, and 1 mm gaps between the end of each glass rod and the reflecting mirror. The layout discussed in Sec. 6.2, which has no gaps between the beamsplitter and glass rods, would require an optical bond between the surface of the beamsplitter and the face of the glass rod. Optical bonding is a difficult process that can potentially have low yield, and therefore an alternate approach is advantageous to reduce the complexity and increase the production quality of the assembly. Spacer gaps between the two surfaces allow each face to be anti-reflective (AR) coated (reducing loss at the beamsplitter/glass rod interface) and greatly simplifies the assembly process. Symmetric gaps between the beamsplitter and glass rods do not contribute to the OPD and expansion/contraction of the substrate due to temperature changes will also be symmetric across each spacer gap.

Similarly, 1 mm air gaps have been inserted between the end of the glass rods and mirrors. Small misalignments due to polishing and machining tolerances can degrade the quality of beam overlap at the beamsplitter. To mitigate misalignment due to processing tolerances a kinematic mirror is used in long arm reflector with a 1 mm air gap. However, an air gap will change the OPD slightly and, more importantly,

degrade the thermal compensation and angular bandwidth. Adding an equal 1 mm air gap to the reflector of the short arm glass rod cancels the OPD shift and preserves the good thermal and wide-angle properties because, as stated above for the spacer gaps, the gaps are equal and therefore thermal expansion will be matched in each arm. The additional air gaps due to the spacers and mirror gaps therefore do not invalidate the mathematical analysis from Sec. 6.2.

The beam entry and exit points at the beamsplitter surface are simulated with Zemax and are used in the CAD model for layout and positioning. A single kinematic mirror directs the beam from the collimator input to the beamsplitter. This input kinematic mount enables fine adjustments of the AOI at the input of the interferometer. One arm of the interferometer has an adjustable mirror to compensate for small misalignments due to imperfect machining and polishing. The other arm has a fixed mirror. The output beams are directed to fiber couplers with at least two kinematic mirror mounts. Four degrees of freedom are needed to control the beam position and angle as it enters the coupler, and therefore two kinematic mounts are required.

6.5 Measurement Results and Discussion

The performance of the interferometer is verified using optical beams with single-mode (SM) and multi-mode (MM) intensity profiles. Atmospheric turbulence is emulated by mode mixing in a multi-mode fiber (Ursin et al., 2007; Jin et al., 2018). The experimental setup, shown schematically in Fig. 6.8, consists of a continuous-wave laser diode (Fitel F0L15DCWC) operating at 1550 nm with a laser controller (Arroyo 6310 Combo Source) that controls the diode current and the temperature of the package. The wavelength of the output for diodes of this type is a function of the bias current and temperature. The controller has an analog voltage input for manual adjustment of the current supplied to the laser diode. A controllable voltage

source is used as the scan voltage input for diode current sweeps. The light from the laser is directed to the interferometer via a single or multi-mode optical fiber. Adhesive heater tape (Omega KHLVA-101/5-P) is attached to the short arm glass to provide phase tuning control of the interference. The output of the interferometer is coupled in to an optical fiber where the output power is measured with an optical power meter (Newport Optical Power Meter 1803C with Model 818-IG sensor head), or the intensity profile of the beam can be viewed with a beam profiling camera (Ophir-Spricon SP907-1550).

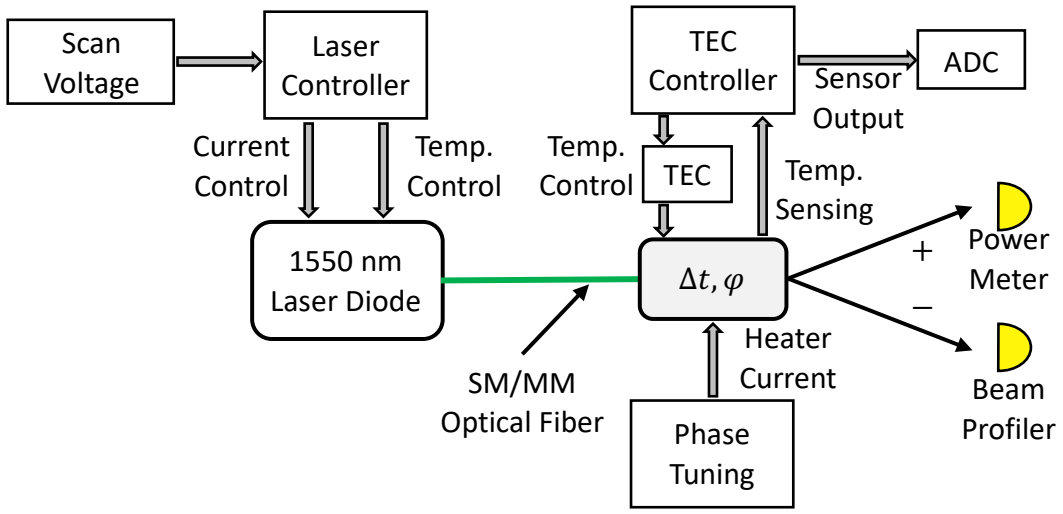

FIGURE 6.8: Schematic of the interferometer experimental setup.

In a field deployment the interferometer's temperature is meant to be passively controlled by modest isolation from fluctuations in the surrounding lab environment. For the purposes of thermal characterization (discussed below) the experimental setup includes precise temperature control with thermo-electric cooling elements (TEC, Laird 64975-502) and a TEC controller (Thorlabs TED200C) with proportional-integral-derivative (PID) feedback control. Three TEC elements are

placed between the bottom of the interferometer base plate and a large thermal bath, which is the optical table in this case. The temperature of the base plate is sensed via high-accuracy thermistors (Vishay NTCALUG02A103F161) placed at various locations on the plate. The thermistor near the center of the plate is used for the TEC feedback control. The analog output from the TEC controller is digitized with an analog-to-digital converter (ADC, National Instruments NI-9239) and recorded. A representative example of the settling time and temperature stability of the interferometer is shown in Fig. 6.9.

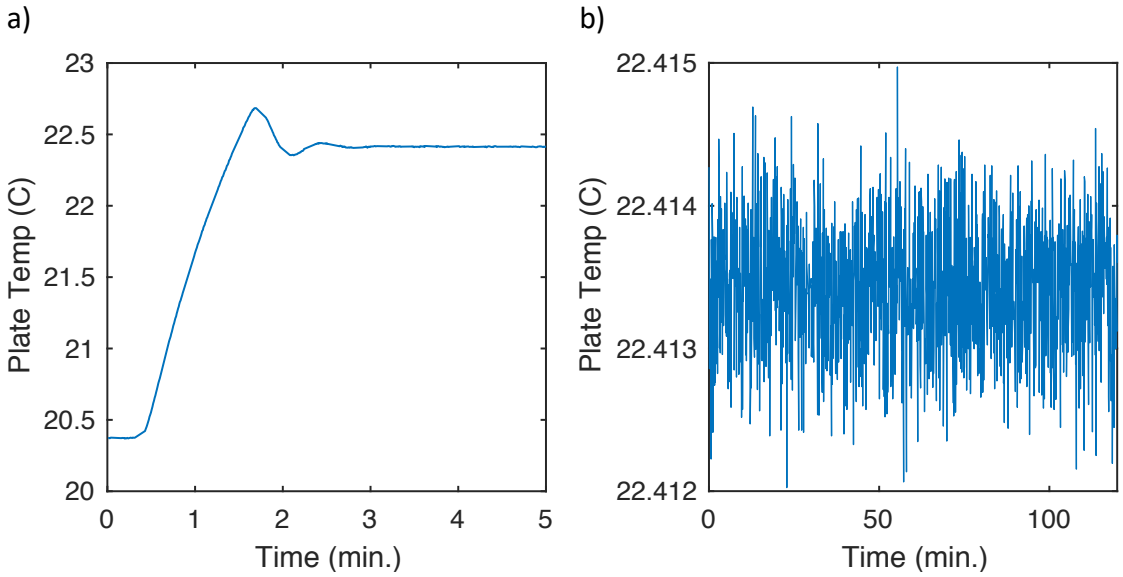

FIGURE 6.9: Temperature control of the interferometer bottom plate. (a) Settling time of the plate temperature after a step change of 2 °C. The target temperature is stable after ∼ 3 minutes. (b) Long-term temperature stability at a fixed set point. The temperature is controlled with an accuracy of ±0.0015 °C.

6.5.1 Interference Characterization

The phase of the interference fringe is scanned by heating one of glass arms as discussed above and shown in Fig. 6.10. To maintain repeatability and execute measurements on faster timescales than thermal settling allows, interference fringes

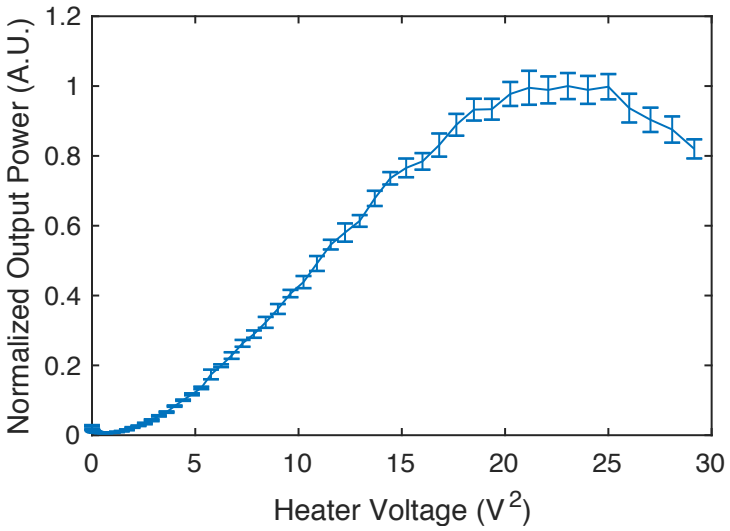

FIGURE 6.10: Interference phase tuning with short arm temperature control. The output from the interferometer is plotted as a function of the square of the voltage supplied to the heater element on the short arm showing a tuning range over a full interference fringe.

are recorded by scanning the input wavelength rather than scanning the phase of the interferometer. The wavelength of the laser diode is adjusted with an analog voltage input to the laser controller which controls the current supplied to the diode. As the laser current is scanned the wavelength changes but so too does the total output power. The output power as a function of the laser current is first calibrated by measuring the power directly from the fiber. The power shift is then subtracted from interference fringe measurements. The output of the the interferometer is measured as a function of the input scan voltage value. As introduced in Chapter 2, the quality of the interference is quantified by the visibility $\mathcal{V}$, given by

$$\mathcal{V} = \frac{\mathcal{P}_+ - \mathcal{P}_-}{\mathcal{P}_+ + \mathcal{P}_-}, \tag{6.9}$$

where $\mathcal{P}_+$ is the maximum and $\mathcal{P}_-$ is the minimum value of the interference fringe.

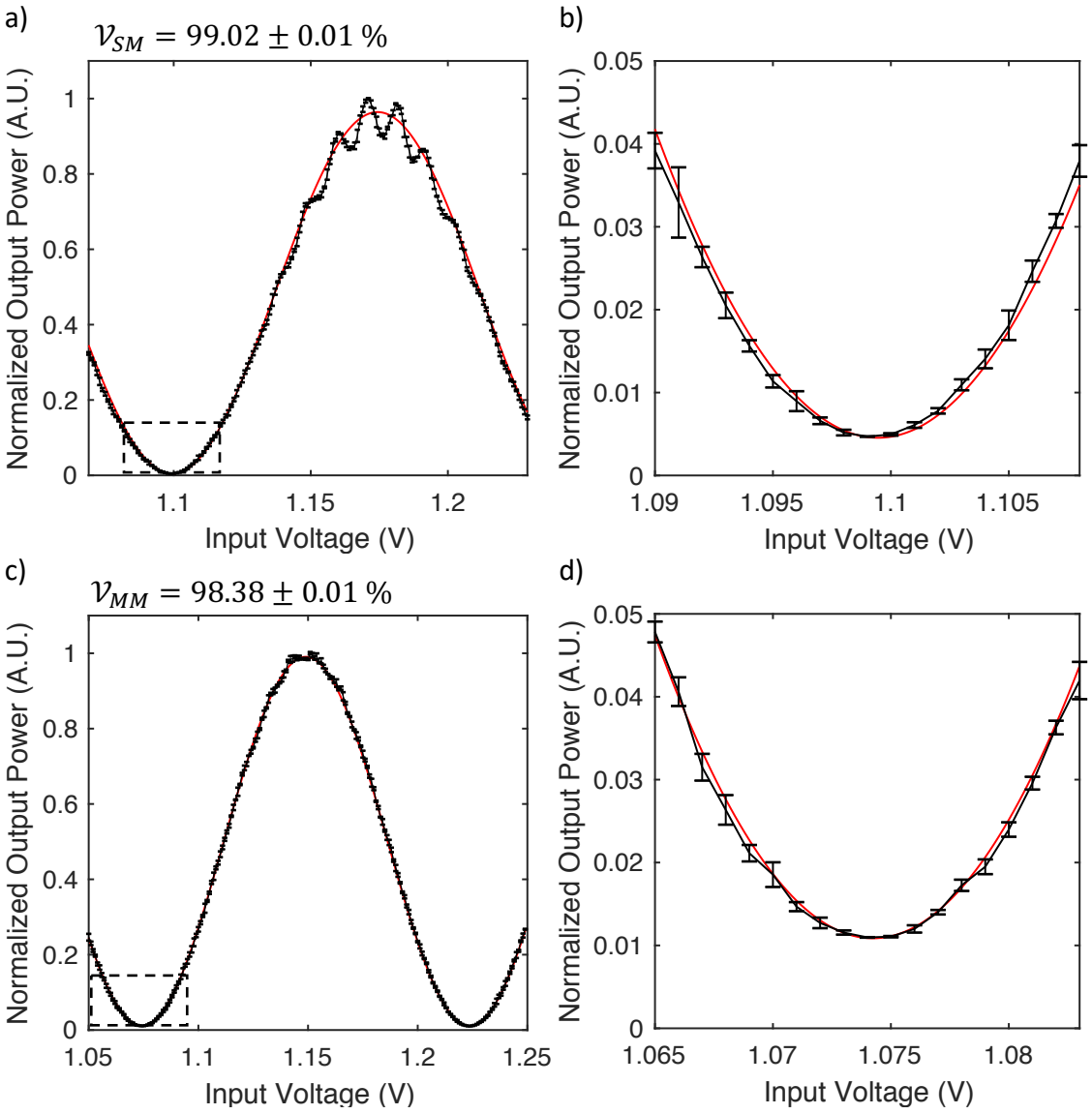

FIGURE 6.11: Interference fringes for SM and MM (50 μm core fiber) input beams as a function of the input voltage to scan the laser diode current. Each data point (black) is the average of 10 measurements and error bars indicate the standard deviation of those 10 measurements. Red lines show a fit to the data using the function given by Eq. 6.10. (a) SM interference fringe. The visibility of the interference is $\mathcal{V}_{SM} = 99.02 \pm 0.01\,\%$. The high order fringe structure in the constructive interference section could be due to a slight misalignment in the overlap of the beam. (b) Zoomed view of the SM fringe minimum. (c) MM interference fringe. The visibility of the interference is $\mathcal{V}_{MM} = 98.38 \pm 0.01\,\%$. (d) Zoomed view of the MM fringe minimum.

The normalized power $P_{out,\pm}$ measured at the $+/-$ port of the interferometer when the phase of the interference is ϕ as a function of small changes of the wavelength $\delta\lambda \ll \Delta$ is given by (Islam et al., 2017b)

$$\frac{P_{out,\pm}}{P_0} = \frac{a}{2}\left[1 \mp \sin\left(k\delta\lambda + \phi\right)\right] + b, \tag{6.10}$$

where P_0 is the input optical power, $a \in \{0, 1\}$ is the insertion loss of the interferometer, b accounts for imperfect destructive interference in the minimum of the fringe, and $k = 2\pi/\lambda$ is the wavenumber of the light. The output power is recorded as a function of the laser diode scan voltage which serves as the phase adjustment of the fringe. The fringe measurement is fit with a curve given by Eq. 6.10 where a, b, and ϕ are free parameters. The visibility of the normalized fringe is extracted from this fit where

$$\mathcal{V} = \frac{a}{a + 2b} \tag{6.11}$$

The interference measurement results from a single-mode input fiber (Corning SMF-28-Ultra) and multi-mode input fiber (50 μm core, Coastal Connections M-FUFU-50sL) are shown in Fig. 6.11. The interferometer demonstrates single-mode interference visibility $\mathcal{V}_{SM} = 99.02\,\%$ and multi-mode interference visibility $\mathcal{V}_{MM} = 98.38\,\%$ extracted from the fitted functions. The single-mode results are close to those reported by high-performing commercial interferometers such as those used in the QKD demonstration (Islam et al., 2017b). Additionally, the multi-mode results presented here are several percent higher than those recently reported for multi-mode interference in other groups (Zeitler et al., 2016; Jin et al., 2018).

6.5.2 Spatial Mode Performance

A robust multi-mode interferometer is required to maintain high visibility independent of the input spatial mode structure. The multi-mode results presented above were optimized and performed on a single profile. To characterize the multi-mode performance of the interferometer I characterize the visibility of the interference fringe for different spatial profiles. The interference is optimized for the first spatial profile and measured for subsequent profiles where the difference between the two spatial modes is quantified by the two dimensional Pearson correlation coefficient. The correlation coefficient R between two matrices (measured intensity as a function of the spatial position, in this case) at time t_1 and t_2 is defined as

$$R = \frac{\sum_{i=1}^{N_x} \sum_{j=1}^{N_y} \left[I_{ij}\left(t_1\right) - \mu\left(t_1\right) \right] \left[I_{ij}\left(t_2\right) - \mu\left(t_2\right) \right]}{\sigma(t_1)\sigma(t_2)}, \tag{6.12}$$

where $I_{ij}(t_n)$ is the optical intensity collected at time t_n (a frame), indexed by a discrete array with positions (i, j) that are the pixels of the camera, $\mu\left(t_n\right)$ is the mean intensity, and $\sigma(t_n)$ is the standard deviation of the intensity distribution. The value of R has a value between $+1$ and -1, where $+1$ indicates perfect positive correlation and -1 indicates a perfect negative correlation and values close to 0 indicate no correlation.

Optical intensity profiles are collected by the beam profiling camera and the autocorrelation is processed in MATLAB. The spatial mode of the beam is changed by introducing a controlled bend in the optical fiber with a micrometer and positioning stage. A schematic depicting the setup to induce changes in the mode is shown in Fig. 6.12a. The fiber is anchored at three different points with the middle point on the positioning stage. As the position of the stage is adjusted the fiber is bent at two different points and changes in the bend cause the mode to change. Special care

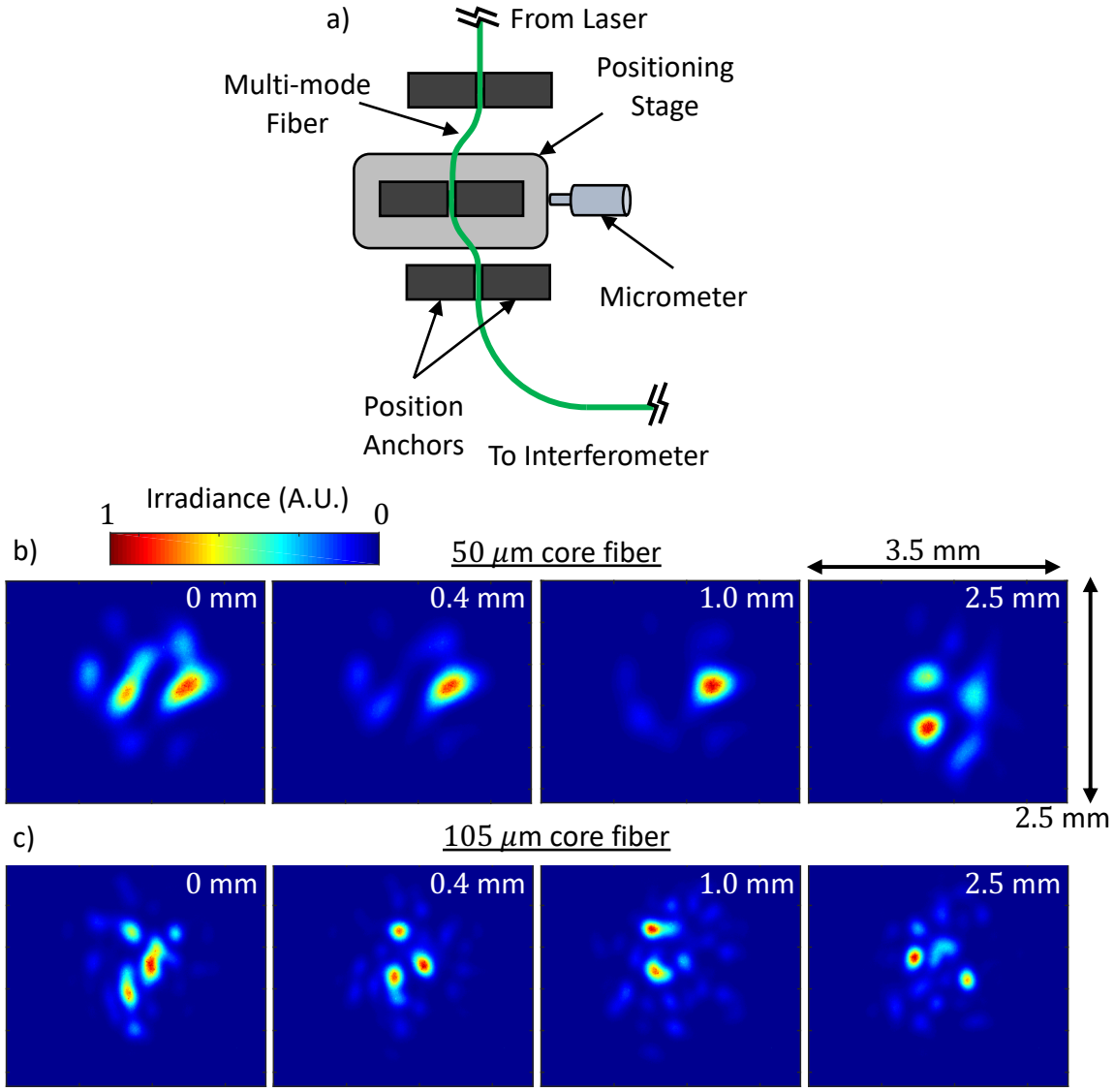

FIGURE 6.12: Spatial mode characterization from a 50 μm and 105 μm core fiber. (a) Schematic showing the setup used to adjust the mode profile of the beam. The spatial mode is changed by inducing bends in the fiber controlled by a positioning stage and a micrometer. (b) Spatial mode examples for different micrometer settings (white text) from a 50 μm core fiber. (c) Spatial mode examples for different micrometer settings (white text) from a 105 μm core fiber.

is taken to ensure that all other points in the fiber are stationary. When the fiber is kept secure apart from the micrometer adjustment, the specific spatial modes can be reproduced depending on the position of the micrometer.

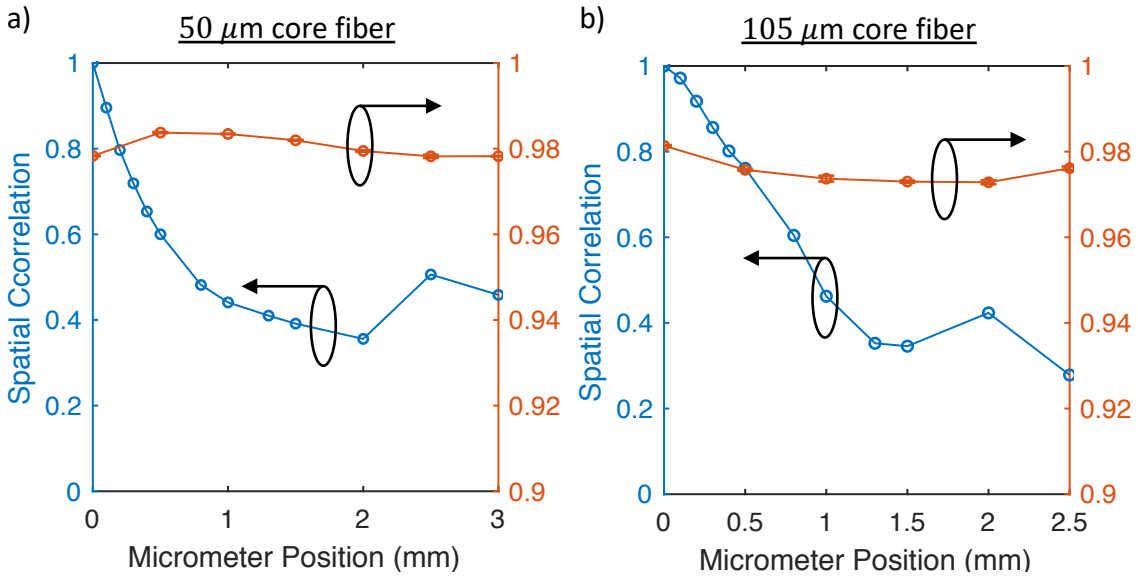

FIGURE 6.13: Multi-mode interference as a function of the input spatial mode. Normalized autocorrelation between the first frame and subsequent frames as a function of the micrometer setting for (a) 50 μm and (b) 105 μm core fiber. Also plotted is the visibility of the interference fringe over the same micrometer range for each fiber.

The beam profile is measured from the output of the fiber (with no collimation) using the beam profiler. Examples of the intensity patterns from 50 μm and 105 μm core (Thorlabs FG105LVA) fibers for different micrometer positions are shown in Fig. 6.12b-c. Note that the experiment is carried out by first recording the mode profiles with the beam profiler at each micrometer position, then performing the interference measurements at each micrometer position. Between the beam profiler measurements and the interference measurements the output of the fiber must be moved from the beam profile to the interferometer input. The movement of the fiber will unavoidably change the actual spatial mode that travels through the interferometer from those in the recorded images in Fig. 6.12b-c. However, the intensity profile, and moreover the *correlation* between profiles at different micrometer positions recorded by the beam profiler are representative of the actual mode passing through the interferometer. Therefore, the mode analysis using the beam profiler

accurately represents the spatial mode at the input of the interferometer.

The correlation coefficient and interference visibility as a function of micrometer position is shown in Fig. 6.13. The autocorrelation between the first measurement and subsequent measurements decays to a value approaching 0 as the spatial mode becomes more distinguishable. As the spatial mode is changed the interferometer maintains excellent fringe visibility for each input fiber measured. The quality of the interference using a 50 μm core fiber has an average value $\mathcal{V}_{avg} = 98.05 \pm 0.01\%$ and a maximum value $\mathcal{V}_{max} = 98.38 \pm 0.01\%$. Additionally, the quality of the interference using a 105 μm core fiber has an average value $\mathcal{V}_{avg} = 97.55 \pm 0.04\%$ and a maximum value $\mathcal{V}_{max} = 98.14 \pm 0.02\%$. The results of these measurements indicate a high-quality of interference that is robust for arbitrary input spatial modes.

6.5.3 Thermal Performance

The thermal performance of the interferometer is characterized by measuring the visibility of the interference fringe and the path length shift as a function of temperature. The temperature of the bottom plate is controlled by the TEC controller which supplies current to the TEC elements in contact with the bottom plate of the interferometer. Once the temperature is changed the system is allowed to come to thermal equilibrium after a period of $\sim$ 30 minutes. As thermal equilibrium is reached the path length will drift as a function of time, causing a change in the output power. Therefore, the output of the interferometer is monitored as equilibrium is reached. Once the output power has stabilized it is determined that the interferometer has come to thermal equilibrium. Ideally, the phase of the interference should set such that it lies on the point of the steepest slope during the settling time in order to have the maximum sensitivity in the output power. A high sensitivity helps determine if the interferometer has come into thermal equilibrium. The equilibrium settling determination is done manually, though there is opportunity for automation.

An example of the equilibrium time for a step change in temperature is shown in Fig. 6.14.

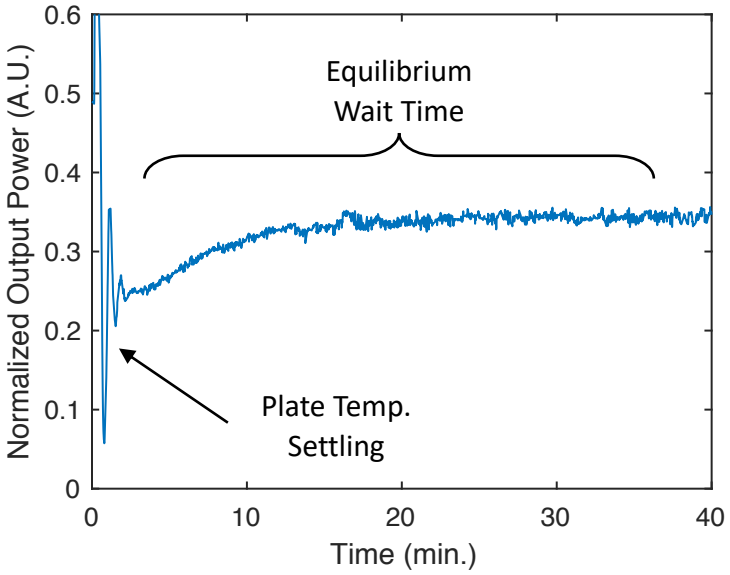

FIGURE 6.14: Example measurement of the output power from the interferometer while the system reaches thermal equilibrium. This particular set of data shows a temperature change from 21.0°C to 21.5°C

Once the system has come to thermal equilibrium a full interference fringe is scanned in the same manner as discussed above and fitted with the function given by Eq. 6.10. A fringe is recorded at each temperature setting and plotted as a function of the scanning voltage applied to the diode controller. The results of the curve fitting are shown in Fig. 6.15. Path length drift brought on by the temperature change causes the fringe to move horizontally. When operating at a set value of ϕ (shown by the 'X' on the yellow curve in the figure) a horizontal shift of the fringe will manifest in a change in the power measured at the output port of the interferometer. The change in output power describes change in path length.

The path length change and visibility are measured for a temperature range of ± 1.0°C centered at 22.0°C. The results of the measurements are shown in Fig. 6.15.

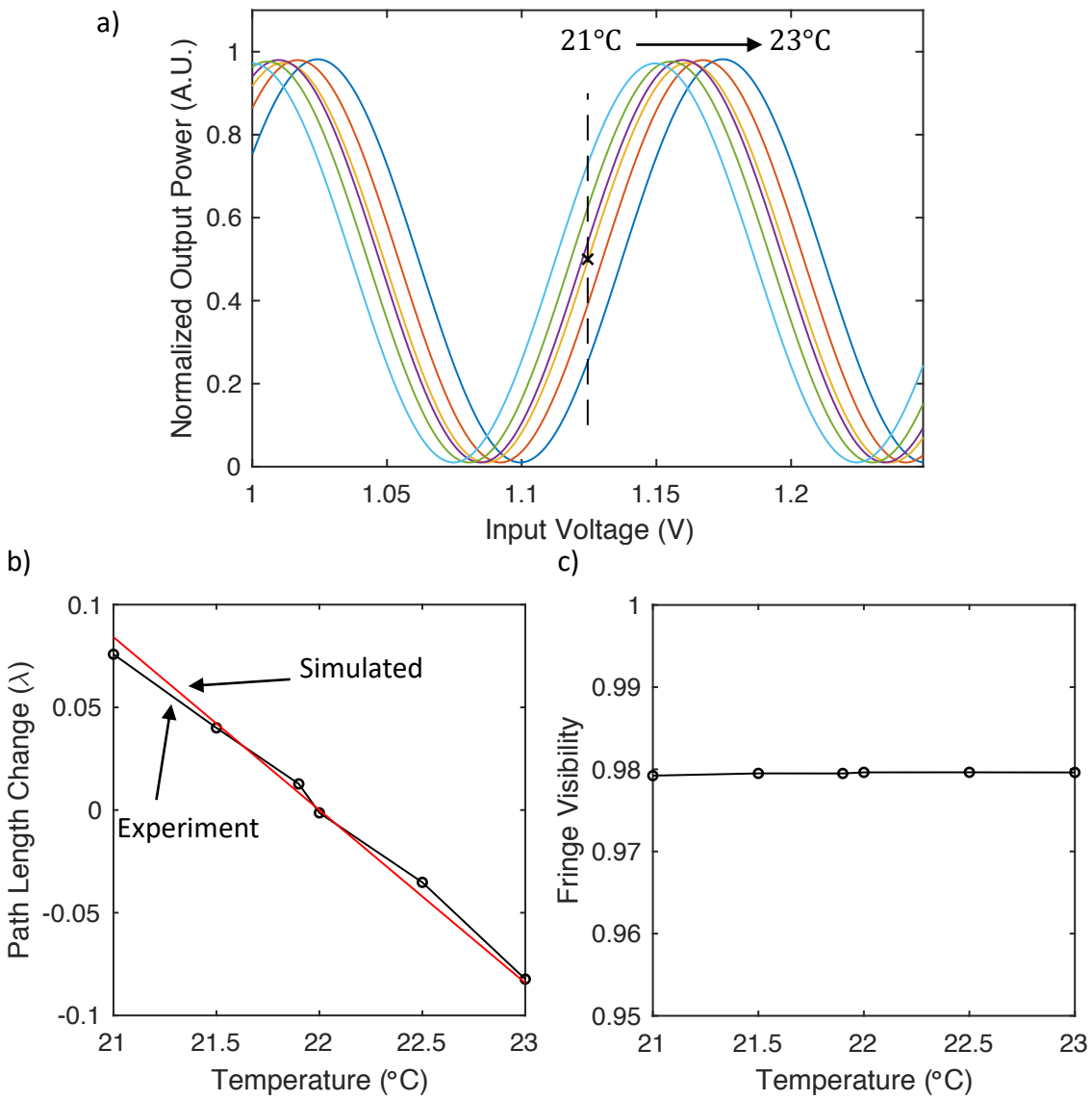

FIGURE 6.15: Multi-mode interference as a function of temperature for temperature values of $21.0, 21.5, 21.9, 22.0, 22.5$, and $23.0\,^{\circ}$C. The $22.1\,^{\circ}$C data point is excluded because of a malfunction in the data acquisition. (a) Fitted functions to the measured interference fringe at each temperature setting. The temperature settings for the curves moving from left to right are $21.0, 21.5, 21.9, 22.0, 22.5$, and $23.0\,^{\circ}$C. The phase of the interference at $22.0\,^{\circ}$C is set at data point marked with an 'X.' The path length shift is calculated using points where the fringe intersects the dotted line. (b) Experimentally measured (black) and theoretically predicted (red) path length change as a function of temperature. (c) Interference visibility as a function of temperature.

A high fringe visibility of $\sim 98\,\%$ is maintained across the entire temperature range. The experimentally determined path-length shift as a function of temperature is $130\,\mathrm{nm}/^{\circ}\mathrm{C}$. This value matches well with the theoretically predicted performance. Therefore stability on the order of $\lambda/50$ can be achieved with moderate temperature control in a lab environment on the order of $0.25\,^{\circ}\mathrm{C}$.

6.6 Conclusion and Future Measurements

In this chapter I have described the framework and necessary characterization to construct a free-space optical link for quantum communication, and specifically in the development of a robust multi-mode time-delay interferometer. Spatial mode scrambling caused by atmospheric turbulence necessarily requires the design of a communications receiver to support many spatial modes. Atmospheric simulations performed via a method that uses discrete phase screens to emulate turbulence effects. Using the results of the simulations I am able to characterize the beam properties, namely the size and divergence of the beam, after free-space propagation. The results of this analysis indicate that multi-mode fiber coupling at the receiver is possible to achieve with geometric loss under the maximum threshold for our time-phase QKD scheme. Fiber coupling from the free-space channels allows a more pragmatic approach to the interferometer design that decouples the input of the interferometer from the receiver optics.

I then detail the design methodology and performance simulations of a time-delay interferometer with a 5 GHz free-spectral-range (200 ps time-delay). The interferometer consists of a Michelson-type layout with glass beam paths in each arm. A wide field-of-view and excellent thermal stability can be achieved with a proper material and dimension choice while satisfying the target time-delay. Finally, I describe the construction and performance of the interferometer. The performance results are highlighted by a maximum interference visibility for single-mode

$\mathcal{V}_{SM} = 99.02 \pm 0.01\,\%$ (comparable to commercial single-mode products) and multi-mode $\mathcal{V}_{MM} = 98.38 \pm 0.01\,\%$ (several percent higher than recent reports). Additionally, multi-mode visibility $\mathcal{V}_{MM} \approx 98\,\%$ is maintained independent of spatial mode profile for both $50\,\mu$m and $105\,\mu$m core fibers. Lastly, high-quality interference is maintained over a modest temperature range of $\pm 1\,^{\circ}$C. The path-length shift of the interferometer is $130\,\mathrm{nm}/\,^{\circ}\mathrm{C}$, enabling excellent thermal stability with modest temperature control.

Future experiments include performing the phase-state measurements with single-mode and multi-mode optical beams. A multi-mode phase-state measurement would require the use of a large area detector. SNSPDs with active areas of $\sim 50\,\mu$m have already been developed for other applications utilizing multi-mode fibers (Crain et al., 2019). One concern regarding the phase-state measurement is the actual timing delay of the interferometer. Due to unforeseen difficulties in the processing of the glass rods the final lengths are short by $\sim 0.6\,$mm in the long arm, and $\sim 0.4\,$mm in the short arm. For the data presented in this chapter I was able to compensate for these mistakes by adjusting the position of the reflector in the long arm in order to preserve the designed angular bandwidth and thermal stability, but this came at the expense of the time delay. I estimate that the time delay after the compensation is $\sim 198\,$ps, which is $2\,$ps shorter than the target value of $200\,$ps. The reduced time-delay will result in an imperfect overlap of the two time-bins in the phase state which are separated by $200\,$ps, and therefore degrade the visibility of this interference. The extent of this degradation in visibility is yet to be investigated.

7

Conclusion

Quantum engineering is an emerging industry that will have a profound impact on future methods of computation and communication. A world-wide effort has been underway for better than a decade to develop quantum enabled technologies including quantum computers and quantum communication systems. The demonstration of a fault-tolerant quantum computer will be a disruptive breakthrough with significant implications to technology, business, and most importantly to communication. Current methods of encrypted communication based on public key encryption would be rendered useless to a functioning quantum computer. Quantum key distribution is an important practical application that enables provably secure distribution of cryptographic keys over an insecure communication channel, even in the presence of an eavesdropper with a quantum computer. The development of QKD systems that operate near the current rate of communication are becoming increasingly important to develop as the once far-off dream of a quantum computer is becoming a realistic expectation.

7.1 Thesis Summary

This thesis describes the development of key technologies that enable the development of high-rate, free-space quantum communication systems. My contribution to the field of quantum communication includes the optimization of a robust quantum receiver that enables communication protocols such as time-phase QKD over a free-space channel. Chapter 2 describes the details of the time-phase protocol that allows for a high bit-rate communication in the presence of detector count-rate saturation. The time-phase protocol is a high-dimensional encoding that enables a single-photon to encode many bits of information. High-dimensional schemes are great candidates for communication protocols operating at high rates and in the presence of loss and detector saturation.

In Chapter 3 I discuss the necessary infrastructure required to operate high-performing single-photon detectors, SNSPDs. The performance of SNSPDs is often hindered by a sub-optimal electrical read-out scheme. In Chapter 4 I describe the development of low-noise, low-power cryogenic amplifiers which greatly improve the timing and count rate performance of SNSPDs. The results of the amplifier circuits boast maximum counts rates exceeding 20 Mcps and timing-jitter as low as 35 ps. The scalable cryogenic read-out circuit coupled with high-efficiency SNSPDs enabled a record-setting secret key rate of 26.2 Mbit/s to be achieved in a proof-of-principle time-phase QKD protocol.

Chapter 5 describes a new mode of operation for conventional single-pixel SNSPDs where the traditional Geiger mode of detection is extended to multi-photon resolution. In this work I experimentally demonstrate that multi-photon detection in conventional SNSPDs is possible where the number of detected photons is encoded in the rise-time of the detection waveform. The results of this investigation are highlighted by multi-photon detection of up to four photons and an extremely low BER

for discriminating detection events between $n = 1$ and $n > 1$. Additionally, our experimental findings are supported by a universal model describing the dynamics of SNSPD detection.

My final contribution to quantum communication system development is the extension of the fiber-based time-phase protocol to free-space communication links with the development of a multi-mode time-delay interferometer. Atmospheric turbulence causes spatial mode scrambling of the optical beam and therefore the receiver, and most importantly the time-delay interferometers used in the phase-basis measurement, must also support many spatial modes. In Chapter 6 I detail the design of a field-widened, a-thermal interferometer with a free spectral range of 5 GHz (time-delay of 200 ps). The results of the interferometer feature interference visibility for single-mode beams of 99 % and multi-mode interference visibility > 98 %. Additionally, multi-mode visibility $\mathcal{V}_{MM} \approx 98\,\%$ is maintained independent of spatial mode profile and over a modest temperature range of $\pm 1\,^{\circ}\mathrm{C}$. The path-length shift of the interferometer is $130\,\mathrm{nm}/\,^{\circ}\mathrm{C}$, enabling excellent thermal stability with modest temperature control.

7.2 Future Directions

Quantum communication systems have progressed at an incredible rate since the first QKD demonstration in 1989. The future for schemes of this type depend upon increasing the rate of communication and filling the need of specialized applications. The communication rate continues to be bottled-necked by the slow recovery time of single-photon detectors. Further development of high-speed detectors with novel read-out circuits to reduce the detector recovery time is important for limiting the effect that detector saturation has on the communication rate. Additionally, increasing the channel capacity using high-dimensional schemes can potentially be enhanced using a photon-number resolving detector. The number resolving power of single-pixel

SNSPDs is very new and potentially has the opportunity for further optimization in the detector design and read-out circuit to increase the number resolution and extend the sensitivity to higher photon numbers. Number resolution could also contribute to an increased channel capacity for quantum communication, or aide in the security of QKD schemes using weak coherent states. Additionally, photon-number resolving detectors are important tools for general quantum optics experiments such as source characterization. Finally, the multi-mode interferometer has demonstrated great performance but can still be improved. Currently the phase tuning relies on thermal time-scales and is therefore very slow. Other schemes can be considered such as stable mechanical tuning methods to enable faster fringe scanning. This can be especially advantageous for protocols where the transmitter might be on a moving platform and doppler effects must be compensated in the interferometer.

Appendix A

Time-Delay Interferometer Derivations

This appendix details the mathematical derivations of the multi-mode interferometer discussed in Chapter 6. The calculations shown below closely follow those by Shepherd et al. (1985) and Gault et al. (1985). In the referenced papers the authors perform a Taylor expansion of the generalized optical path difference about normal incidence. My calculations perform the expansion about a finite angle and carry out the rest of the analysis in a similar manner as the referenced papers with deviations in the analysis pointed out where applicable.

A.1 Constraint Derivations

The interferometer is constructed with a balanced beamsplitter cube where the two outputs of the beam splitter are directed to two arms of a Michelson-type setup. A short path is comprised of glass with length d_1 and index of refraction n_1, and a long path with glass of length d_2 and index of refraction n_2. An optional air gap can be added at the end of one or both glass beam paths before the reflecting surface. In this analysis I will include an air gap of length d_3 and material n_3. The material n_3

will be vacuum but for now the equations are kept the most general form.

The OPD Δ as a function of the input angle θ is given by,

$$\Delta/2 = [n_3 d_3(1-\sin^2\theta/n_3^2)^{1/2} + n_2 d_2(1-\sin^2\theta/n_2^2)^{1/2} - n_1 d_1(1-\sin^2\theta/n_1^2)^{1/2}] \quad \text{(A.1)}$$

Then, I perform an expansion of $(1-\sin^2\theta/n_i^2)^{1/2}$ about a fixed offset angle $\Phi = \sin\theta_0$. Defining the effective index of refraction $\beta_i^2 = n_i^2 - \Phi^2$ the Taylor expansion is written as,

$$(1-\sin^2\theta/n_i^2)^{1/2} = \frac{1}{n_i}\beta_i - \frac{\Phi}{n_i\beta_i}(\sin\theta-\Phi) - \frac{n_i^2}{2n_i\beta_i^3}(\sin\theta-\Phi)^2 + \cdots \quad \text{(A.2)}$$

$$\pm n_i d_i(1-\sin^2\theta/n_i^2)^{1/2} = \pm\,(d_i\beta_i) \mp \frac{\Phi d_i}{\beta_i}(\sin\theta-\Phi) \mp \frac{n_i^2 d_i}{2\beta_i^3}(\sin\theta-\Phi)^2 + \cdots \quad \text{(A.3)}$$

Inserting the expansion in Eq. A.1 and combining like terms in $(\sin\theta-\Phi)$ I am able to arrive at the expression,

$$\begin{aligned}\Delta/2 = (d_3\beta_3 + d_2\beta_2 - d_1\beta_1) - \Phi(\sin\theta-\Phi)\left(\frac{d_3}{\beta_3}+\frac{d_2}{\beta_2}-\frac{d_1}{\beta_1}\right) \\ -\frac{(\sin\theta-\Phi)^2}{2}\left(\frac{n_3^2 d_3}{\beta_3^3}+\frac{n_2^2 d_2}{\beta_2^3}-\frac{n_1^2 d_1}{\beta_1^3}\right)+\cdots\end{aligned} \quad \text{(A.4)}$$

This equation is the analog to Eq. 23 in Shepherd et al. (1985). The optimization of the interferometer begins with two constraints that are derived from this equation.

A.1.1 Optical Path Difference

The OPD at the central input angle of $\sin\theta = \Phi$ is defined as,

$$\Delta/2 = d_3\beta_3 + d_2\beta_2 - d_1\beta_1. \quad \text{(A.5)}$$

where the delay is given in units of length. Dividing Eq. A.5 by the vacuum speed of light c will give the OPD in units of time, as shown in the body of the main paper in Eq. 6.3.

A.1.2 Field Widening

The OPD is made first-order insensitive to deviations of the input angle by choosing material and path lengths to make the second term in Eq. A.4 vanish. This is the field-widening condition and is given by,

$$\frac{d_3}{\beta_3} + \frac{d_2}{\beta_2} - \frac{d_1}{\beta_1} = 0. \tag{A.6}$$

A.1.3 Thermal Compensation

The third condition to satisfy is passive thermal stability. The physical length and index of each glass is affected by changes in temperature and will change the optical path of each arm. A proper choice in material will make the change in each arm equal and therefore not change the OPD. My analysis of the thermal drift differs slightly from that by Shepherd et al. (1985), and I will describe those differences below.

Thermal stability is analyzed by differentiating the OPD in Eq. A.5 (looking at only the central ray where $\sin\theta = \Phi$) with respect to temperature.

$$\frac{\partial}{\partial T}\left[\Delta = 2\left(d_3\beta_3 + d_2\beta_2 - d_1\beta_1\right)\right], \tag{A.7}$$

$$\frac{\partial \Delta}{\partial T} = 2\left(\beta_3\frac{\partial d_3}{\partial T} + d_3\frac{\partial \beta_3}{\partial T} + \beta_2\frac{\partial d_2}{\partial T} + d_2\frac{\partial \beta_2}{\partial T} - \beta_1\frac{\partial d_1}{\partial T} - d_1\frac{\partial \beta_1}{\partial T}\right). \tag{A.8}$$

Beam path #3 is air and therefore has negligible index changes with temperature. However, temperature changes could change the path length dependent upon the

mounting geometry of the reflecting mirror at the end of the arm. A mirror attached to the glass rod via spacers made of ultra-low expansion (ULE) material will keep the air gap thickness constant with temperature. A mirror that is mounted to a substrate will move as the substrate expands or contracts, and thus will change the air gap thickness. In my analysis, I treat the air gap thickness as constant to arrive at the same result as Shepherd *et al.*

Differentiating Eq. A.4 with respect to temperature gives,

$$\frac{\partial \Delta}{\partial T} = 2\left[\beta_2\left(\frac{\partial d_2}{\partial T}\right) + \frac{d_2 n_2}{\beta_2}\left(\frac{\partial n_2}{\partial T}\right) - \beta_1\left(\frac{\partial d_1}{\partial T}\right) - \frac{d_1 n_1}{\beta_1}\left(\frac{\partial n_1}{\partial T}\right)\right], \tag{A.9}$$

where $\partial\beta_i/\partial T = (1/\beta_i)(\partial n_i/\partial T)$.

Gathering terms in Eq. A.9 and realizing that $\alpha_i = 1/d_i(\partial d_i/\partial T)$ is the coefficient of thermal expansion (CTE) we re-write as,

$$\frac{\partial \Delta}{\partial T} = 2d_2\left[\beta_2\alpha_2 + \frac{n_2}{\beta_2}\left(\frac{\partial n_2}{\partial T}\right)\right] - 2d_1\left[\beta_1\alpha_1 + \frac{n_1}{\beta_1}\left(\frac{\partial n_1}{\partial T}\right)\right]. \tag{A.10}$$

Shepherd *et al.* carries the analysis further and inserts the field-widened condition in to Eq. A.10 to arrive at an a-thermal condition that is independent of the glass path lengths d_1 and d_2. However, I will keep the keep the path lengths in the equation and arrive at the a-thermal condition by setting $\partial\Delta/\partial T = 0$, arriving at,

$$d_2\left[\beta_2\alpha_2 + \frac{n_2}{\beta_2}\left(\frac{\partial n_2}{\partial T}\right)\right] = d_1\left[\beta_1\alpha_1 + \frac{n_1}{\beta_1}\left(\frac{\partial n_1}{\partial T}\right)\right]. \tag{A.11}$$

A.2 Optimization Procedure with Air Gap

This section details the procedure to find the path lengths d_1, d_2, and d_3 that satisfy the target OPD (Eq. A.5), field-widened condition (Eq. A.6), and a-thermal condition

(Eq. A.11).

The procedure begins by combining the OPD (Eq. A.5) and field-widened (Eq. A.6) equations to cancel air-gap thickness d_3 to arrive at one equation with d_2 in terms of d_1 and material parameters. Solving Eq. A.6 for d_3 gives,

$$d_3 = \beta_3 \left(\frac{d_1}{\beta_1} - \frac{d_2}{\beta_2} \right). \tag{A.12}$$

Next, the expression for d_3 is inserted in to the OPD,

$$\Delta/2 = \beta_3^2 \left(\frac{d_1}{\beta_1} - \frac{d_2}{\beta_2} \right) + d_2\beta_2 - d_1\beta_1. \tag{A.13}$$

Combining like terms and simplifying gives,

$$\Delta/2 = d_2\beta_2 \left(1 - \frac{\beta_3^2}{\beta_2^2} \right) - d_1\beta_1 \left(1 - \frac{\beta_3^2}{\beta_1^2} \right). \tag{A.14}$$

Finally, solving for d_2 gives,

$$d_2 = \frac{\Delta/2 + \beta_1 \left(1 - \frac{\beta_3^2}{\beta_1^2} \right) d_1}{\beta_2 \left(1 - \frac{\beta_3^2}{\beta_2^2} \right)}. \tag{A.15}$$

Equation A.15 provides one equation for d_2 in terms of d_1. Additionally, solving the a-thermal condition Eq. A.11 for d_2,

$$d_2 = \left[\frac{\beta_1\alpha_1 + \frac{n_1}{\beta_1} \left(\frac{\partial n_1}{\partial T} \right)}{\beta_2\alpha_2 + \frac{n_2}{\beta_2} \left(\frac{\partial n_2}{\partial T} \right)} \right] d_1, \tag{A.16}$$

provides a second equation for d_2 in terms of d_1. Equations A.15 and A.16 gives values for d_1 and d_2. The air gap thickness is found by substituting d_1 and d_2 in to the OPD.

A.3 Optimization Procedure without Air Gap

This section details the procedure to find the path lengths d_1 and d_2 where the there is no air gap ($d_3 = 0$). In this situation the three constraints discussed above cannot be satisfied simultaneously. Therefore, we satisfy the field-widened and OPD constraints exactly, and approximately satisfy the a-thermal condition.

First, the field-widened condition is solved for d_2, giving,

$$d_2 = \frac{\beta_2}{\beta_1} d_1. \tag{A.17}$$

This equation is then inserted in to the OPD (with $d_3 = 0$),

$$\frac{\Delta}{2} = \beta_2 \left(\frac{\beta_2}{\beta_1} \right) d_1 - \beta_1 d_1. \tag{A.18}$$

After simplification the value of d_1 is given by,

$$d_1 = \left(\frac{\Delta}{2} \right) \frac{\beta_1}{\beta_2^2 - \beta_1^2} \tag{A.19}$$

Lastly, the value of d_2 is found by inserting the value of d_1 in to either the OPD or the field-widened equation.

Bibliography

Agne, S., Kauten, T., Jin, J., Meyer-Scott, E., Salvail, J. Z., Hamel, D. R., Resch, K. J., Weihs, G., and Jennewein, T. (2016), "Observation of genuine three-photon interference," *arXiv preprint arXiv:1609.07508*.

Allman, M. S., Verma, V. B., Stevens, M., Gerrits, T., Horansky, R. D., Lita, A. E., Marsili, F., Beyer, A., Shaw, M. D., Kumor, D., Mirin, R. P., and Nam, S. W. (2015), "A near-infrared 64-pixel superconducting nanowire single photon detector array with integrated multiplexed readout," *Applied Physics Letters*, 106, 192601.

Baek, B., Lita, A. E., Verma, V., and Nam, S. W. (2011), "Superconducting aW x Si 1- x nanowire single-photon detector with saturated internal quantum efficiency from visible to 1850 nm," *Applied Physics Letters*, 98, 251105.

Bardin, J. C. and Weinreb, S. (2009), "A 0.1–5 GHz Cryogenic SiGe MMIC LNA," *IEEE Microwave Wireless Components Letters*, 19, 407.

Barends, R., Kelly, J., Megrant, A., Veitia, A., Sank, D., Jeffrey, E., White, T. C., Mutus, J., Fowler, A. G., Campbell, B., et al. (2014), "Superconducting quantum circuits at the surface code threshold for fault tolerance," *Nature*, 508, 500–503.

Bennett, C. H. and Brassard, G. (1984), "Quantum cryptography: Public key distribution and coin tossing." in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, pp. 175–179.

Bennett, C. H. and Brassard, G. (1989), "Experimental quantum cryptography: the dawn of a new era for quantum cryptography: the experimental prototype is working," *ACM Sigact News*, 20, 78–80.

Bitauld, D., Marsili, F., Gaggero, A., Mattioli, F., Leoni, R., Nejad, S. J., Levy, F., and Fiore, A. (2010), "Nanoscale Optical Detector with Single-Photon and Multiphoton Sensitivity," *Nano Letters*, 10, 2977–2981.

Boroson, D. M., Robinson, B. S., Murphy, D. V., Burianek, D. A., Khatri, F., Kovalik, J. M., Sodnik, Z., and Cornwell, D. M. (2014), "Overview and results of the lunar laser communication demonstration," in *Free-Space Laser Communication and Atmospheric Propagation XXVI*, vol. 8971, p. 89710S, International Society for Optics and Photonics.

Bourgoin, J.-P., Higgins, B. L., Gigov, N., Holloway, C., Pugh, C. J., Kaiser, S., Cranmer, M., and Jennewein, T. (2015), "Free-space quantum key distribution to a moving receiver," *Optics Express*, 23, 33437–33447.

Brougham, T., Barnett, S. M., McCusker, K. T., Kwiat, P. G., and Gauthier, D. J. (2013), "Security of high-dimensional quantum key distribution protocols using Franson interferometers," *Journal of Physics B: Atomic, Molecular and Optical Physics*, 46, 104010.

Brougham, T., Wildfeuer, C. F., Barnett, S. M., and Gauthier, D. J. (2016), "The information of high-dimensional time-bin encoded photons," *European Physics Journal D*, 70, 214.

Bulaevskii, L. N., Graf, M. J., and Kogan, V. G. (2012), "Vortex-assisted photon counts and their magnetic field dependence in single-photon superconducting detectors," *Physical Review B*, 85, 014505.

Cahall, C., Nicolich, K. L., Islam, N. T., Lafyatis, G. P., Miller, A. J., Gauthier, D. J., and Kim, J. (2017), "Multi-photon detection using a conventional superconducting nanowire single-photon detector," *Optica*, 4, 1534–1535.

Cahall, C., Gauthier, D. J., and Kim, J. (2018), "Scalable cryogenic readout circuit for a superconducting nanowire single-photon detector system," *Review of Scientific Instruments*, 89, 063117.

Cattaneo, M., Paris, M. G., and Olivares, S. (2018), "Hybrid quantum key distribution using coherent states and photon-number-resolving detectors," *Physical Review A*, 98, 012333.

Chesnokov, S. S., Kandidov, V. P., Shmalhausen, V. I., and Shuvalov, V. V. (1995), "Numerical/optical simulation of laser beam propagation through atmospheric turbulence." Tech. rep., Moscow State University (USSR).

Cirac, J. I. and Zoller, P. (1995), "Quantum computations with cold trapped ions," *Physical Review Letters*, 74, 4091.

Crain, S., Cahall, C., Vrijsen, G., Wollman, E. E., Shaw, M. D., Verma, V. B., Nam, S. W., and Kim, J. (2019), "High-Speed, Low-Crosstalk Detection of a Trapped 171 Yb $^{+}$ Ion Ancilla Qubit using Superconducting Nanowire Single Photon Detectors," *arXiv preprint arXiv:1902.04059*.

Crain, S. G. (2016), "Integrated System Technologies for Modular Trapped Ion Quantum Information Processing," Ph.D. thesis.

Dauler, E. A., Kerman, A. J., Robinson, B. S., Yang, J. K. W., Voronov, B., Goltsman, G., Hamilton, S. A., and Berggren, K. K. (2009), "Photon-number-resolution

with sub-30-ps timing using multi-element superconducting nanowire single photon detectors," *Journal of Modern Optics*, 56, 364.

Dauler, E. A., Grein, M. E., Kerman, A. J., Marsili, F., Miki, S., Nam, S. W., Shaw, M. D., Terai, H., Verma, V. B., and Yamashita, T. (2014), "Review of superconducting nanowire single-photon detector system design options and demonstrated performance," *Optical Engineering*, 53, 081907.

Divochiy, A., Marsili, F., Bitauld, D., Gaggero, A., Leoni, R., Mattioli, F., Korneev, A., Seleznev, V., Kaurova, N., Minaeva, O., Gol'tsman, G., Lagoudakis, K. G., Benkhaoul, M., Levy, F., and Fiore, A. (2008), "Superconducting nanowire photon-number-resolving detector at telecommunication wavelengths," *Nature Photonics*, 2, 302.

Eisaman, M. D., Fan, J., Migdall, A., and Polyakov, S. V. (2011), "Invited review article: Single-photon sources and detectors," *Review of Scientific Instruments*, 82, 071101.

Ekert, A. K. (1991), "Quantum cryptography based on Bells theorem," *Physical Review Letters*, 67, 661.

Engel, A., Lonsky, J., Zhang, X., and Schilling, A. (2015), "Detection Mechanism in SNSPD: Numerical Results of a Conceptually Simple, Yet Powerful Detection Model," *IEEE Transactions on Applied Superconductivity*, 25, 1–7.

Feynman, R. P. (1982), "Simulating physics with computers," *International Journal of Theoretical Physics*, 21, 467–488.

Gaudio, R., Renema, J. J., Zhou, Z., Verma, V. B., Lita, A. E., Shainline, J., Stevens, M. J., Mirin, R. P., Nam, S. W., van Exter, M. P., de Dood, M. J. A., and Fiore, A. (2016), "Experimental investigation of the detection mechanism in WSi nanowire superconducting single photon detectors," *Applied Physics Letters*, 109, 031101.

Gault, W. A., Johnston, S. F., and Kendall, D. J. (1985), "Optimization of a field-widened Michelson interferometer," *Applied Optics*, 24, 1604–1608.

Google (2019), https://fiber.google.com, Last accessed on 2019-03-12.

Graham, T. M., Bernstein, H. J., Wei, T.-C., Junge, M., and Kwiat, P. G. (2015), "Superdense teleportation using hyperentangled photons," *Nature Communications*, 6, 7185.

Grover, L. K. (1996), "A fast quantum mechanical algorithm for database search," in *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pp. 212–219, ACM.

Guilbert, H. E. and Gauthier, D. J. (2015), "Enhancing heralding efficiency and biphoton rate in Type-I spontaneous parametric down-conversion," *IEEE Journal of Selected Topics in Quantum Electronics*, 21, 215–224.

Hill, A. D., Christensen, B., and Kwiat, P. G. (2016), "Advanced techniques for free-space optical quantum cryptography over water," in *Free-Space Laser Communication and Atmospheric Propagation XXVIII*, eds. D. M. Boroson and H. Hemmati, vol. 9739, SPIE.

Horowitz, P. and Hill, W. (1989), *The Art of Electronics*, Cambridge University Press.

IDQuantique (2019), https://www.idquantique.com, Last accessed on 2019-03-12.

Impagliazzo, R., Levin, L. A., and Luby, M. (1989), "Pseudo-random generation from one-way functions," in *Proceedings of the twenty-first annual ACM symposium on Theory of computing*, pp. 12–24, ACM.

Intallura, P., Ward, M., Karimov, O., Yuan, Z., See, P., Shields, A., Atkinson, P., and Ritchie, D. (2007), "Quantum key distribution using a triggered quantum dot source emitting near 1.3 μm," *Applied Physics Letters*, 91, 161103.

Islam, N. T. (2017), "High-Rate, High-Dimensional Quantum Key Distribution Systems," Ph.D. thesis.

Islam, N. T., Lim, C. C. W., Cahall, C., Kim, J., and Gauthier, D. J. (2017a), "Provably secure and high-rate quantum key distribution with time-bin qudits," *Science Advances*, 3, e1701491.

Islam, N. T., Cahall, C., Aragoneses, A., Lezama, A., Kim, J., and Gauthier, D. J. (2017b), "Robust and Stable Delay Interferometers with Application to d-Dimensional Time-Frequency Quantum Key Distribution," *Physical Review Applied*, 7, 044010.

Islam, N. T., Lim, C. C. W., Cahall, C., Kim, J., and Gauthier, D. J. (2018), "Securing quantum key distribution systems using fewer states," *Physical Review A*, 97, 042347.

Islam, N. T., Lim, C. C. W., Cahall, C., Qi, B., Kim, J., and Gauthier, D. J. (2019), "Scalable high-rate, high-dimensional quantum key distribution," *arXiv preprint arXiv:1902.00811*.

Jin, J., Agne, S., Bourgoin, J.-P., Zhang, Y., Lütkenhaus, N., and Jennewein, T. (2018), "Demonstration of analyzers for multimode photonic time-bin qubits," *Physical Review A*, 97, 043847.

Kaneda, F., Christensen, B. G., Wong, J. J., Park, H. S., McCusker, K. T., and Kwiat, P. G. (2015), "Time-multiplexed heralded single-photon source," *Optica*, 2, 1010–1013.

Kerman, A. J., Dauler, E. A., Keicher, W. E., Yang, J. K. W., Berggren, K. K., GolTsman, G., and Voronov, B. (2006), "Kinetic-inductance-limited reset time of superconducting nanowire photon counters," *Applied Physics Letters*, 88, 111116.

Kerman, A. J., Yang, J. K., Molnar, R. J., Dauler, E. A., and Berggren, K. K. (2009), "Electrothermal feedback in superconducting nanowire single-photon detectors," *Physical Review B*, 79, 100509.

Kerman, A. J., Rosenberg, D., Molnar, R. J., and Dauler, E. A. (2013), "Readout of superconducting nanowire single-photon detectors at high count rates," *Journal of Applied Physics*, 113, 144511.

Kim, J., Takeuchi, S., Yamamoto, Y., and Hogue, H. H. (1999), "Multiphoton detection using visible light photon counter," *Applied Physics Letters*, 74, 902–904.

Kral, L., Prochazka, I., and Hamal, K. (2005), "Optical signal path delay fluctuations caused by atmospheric turbulence," *Optics letters*, 30, 1767–1769.

Kruse, R., Tiedau, J., Bartley, T. J., Barkhofen, S., and Silberhorn, C. (2017), "Limits of the time-multiplexed photon-counting method," *Physical Review A*, 95, 023815.

Lamb, J. W. (2014), "Evaluation of biasing and protection circuitry components for cryogenic MMIC low-noise amplifiers," *Cryogenics*, 61, 43.

Leach, J., Bolduc, E., Gauthier, D. J., and Boyd, R. W. (2012), "Secure information capacity of photons entangled in many dimensions," *Physical Review A*, 85, 060304.

Liao, S.-K., Cai, W.-Q., Liu, W.-Y., Zhang, L., Li, Y., Ren, J.-G., Yin, J., Shen, Q., Cao, Y., Li, Z.-P., Li, F.-Z., Chen, X.-W., Sun, L.-H., Jia, J.-J., Wu, J.-C., Jiang, X.-J., Wang, J.-F., Huang, Y.-M., Wang, Q., Zhou, Y.-L., Deng, L., Xi, T., Ma, L., Hu, T., Zhang, Q., Chen, Y.-A., Liu, N.-L., Wang, X.-B., Zhu, Z.-C., Lu, C.-Y., Shu, R., Peng, C.-Z., Wang, J.-Y., and Pan, J.-W. (2017), "Satellite-to-ground quantum key distribution," *Nature*, 549, 43.

Lo, H.-K., Ma, X., and Chen, K. (2005), "Decoy state quantum key distribution," *Physical Review Letters*, 94, 230504.

Mani, H. and Mauskopf, P. (2014), "A single-stage cryogenic LNA with low power consumption using a commercial SiGe HBT," in *2014 11th International Workshop on Low Temperature Electronics (WOLTE)*, IEEE.

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

Marsili, F., Stevens, M. J., Kozorezov, A., Verma, V. B., Lambert, C., Stern, J. A., Horansky, R. D., Dyer, S., Duff, S., Pappas, D. P., Lita, A. E., Shaw, M. D., Mirin, R. P., and Nam, S. W. (2016), "Hotspot relaxation dynamics in a current-carrying superconductor," *Physical Review B*, 93, 094518.

Migdall, A., Polyakov, S. V., Fan, J., and Bienfang, J. C. (2013), *Single-Photon Generation and Detection: Physics and Applications*, vol. 45, Academic Press.

Miller, A. J., Nam, S. W., Martinis, J. M., and Sergienko, A. V. (2003), "Demonstration of a low-noise near-infrared photon counter with multiphoton discrimination," *Applied Physics Letters*, 83, 791–793.

Miller, A. J., Lita, A. E., Calkins, B., Vayshenker, I., Gruber, S. M., and Nam, S. W. (2011), "Compact cryogenic self-aligning fiber-to-detector coupling with losses below one percent," *Optics Express*, 19, 9102.

Monroe, C. and Kim, J. (2013), "Scaling the ion trap quantum processor," *Science*, 339, 1164–1169.

Montazeri, S., Wong, W.-T., Coskun, A. H., and Bardin, J. C. (2016), "Ultra-low-power cryogenic SiGe low-noise amplifiers: Theory and demonstration," *IEEE Transactions on Microwave Theory Techniques*, 64, 178.

Moshkova, M., Divochiy, A., Morozov, P., Vakhtomin, Y., Antipov, A., Zolotov, P., Seleznev, V., Ahmetov, M., and Smirnov, K. (2019), "High-performance superconducting photon-number-resolving detectors with 86% system efficiency at telecom range," *JOSA B*, 36, B20–B25.

Najafi, F., Marsili, F., Dauler, E., Molnar, R. J., and Berggren, K. K. (2012), "Timing performance of 30-nm-wide superconducting nanowire avalanche photodetectors," *Applied Physics Letters*, 100, 152602.

Nicolich, K. L., Cahall, C., Islam, N. T., Lafyatis, G. P., Kim, J., Miller, A. J., and Gauthier, D. J. (2018), "Universal Model for the Turn-on Dynamics of Superconducting Nanowire Single-Photon Detectors," *arXiv preprint arXiv:1811.01067*.

Nielsen, M. A. and Chuang, I. L. (2010), *Quantum computation and quantum information*, Cambridge University Press.

Pollock, D. H., Accetta, J. S., and Shumaker, D. L. (1993), "The Infrared & Electro-Optical Systems Handbook. Countermeasure Systems, Volume 7," Tech. rep., Infrared Information And Analysis Center, Ann Arbor, MI.

Ren, J.-G., Xu, P., Yong, H.-L., Zhang, L., Liao, S.-K., Yin, J., Liu, W.-Y., Cai, W.-Q., Yang, M., Li, L., Yang, K.-X., Han, X., Yao, Y.-Q., Li, J., Wu, H.-Y., Wan, S., Liu, L., Liu, D.-Q., Kuang, Y.-W., He, Z.-P., Shang, P., Guo, C., Zheng, R.-H., Tian, K., Zhu, Z.-C., Liu, N.-L., Lu, C.-Y., Shu, R., Chen, Y.-A., Peng, C.-Z., Wang, J.-Y., and Pan, J.-W. (2017), "Ground-to-satellite quantum teleportation," *Nature*, 549, 70.

Renema, J. J., Gaudio, R., Wang, Q., Zhou, Z., Gaggero, A., Mattioli, F., Leoni, R., Sahin, D., De Dood, M. J. A., Fiore, A., and Exter, M. P. v. (2014), "Experimental test of theories of the detection mechanism in a nanowire superconducting single photon detector," *Physical Review Letters*, 112, 117604.

Rivest, R. L., Shamir, A., and Adleman, L. (1978), "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, 21, 120–126.

Rosenberg, D., Nam, S. W., Miller, A. J., Salminen, A., Grossman, E., Schwall, R. E., and Martinis, J. M. (2004), "Near-unity absorption of near-infrared light in tungsten films," *Nuclear Instruments Methods in Physics Research Section A: Accelerators, Spectrometers, Detectors and Associated Equipment*, 520, 537.

Rosfjord, K. M., Yang, J. K. W., Dauler, E. A., Kerman, A. J., Anant, V., Voronov, B. M., GolTsman, G. N., and Berggren, K. K. (2006), "Nanowire single-photon detector with an integrated optical cavity and anti-reflection coating," *Optics Express*, 14, 527.

Scarani, V., Bechmann-Pasquinucci, H., Cerf, N. J., Dušek, M., Lütkenhaus, N., and Peev, M. (2009), "The security of practical quantum key distribution," *Reviews of Modern Physics*, 81, 1301.

Schmidt, J. D. (2010), "Numerical simulation of optical wave propagation with examples in MATLAB," SPIE Bellingham, Washington, USA.

Semenov, A. D., Gol'tsman, G. N., and Korneev, A. A. (2001), "Quantum detection by current carrying superconducting film," *Physica C: Supercondivity*, 351, 349.

Shalm, L. K., Meyer-Scott, E., Christensen, B. G., Bierhorst, P., Wayne, M. A., Stevens, M. J., Gerrits, T., Glancy, S., Hamel, D. R., Allman, M. S., et al. (2015), "Strong loophole-free test of local realism," *Physical Review Letters*, 115, 250402.

Shepherd, G. G., Gault, W. A., Miller, D., Pasturczyk, Z., Johnston, S. F., Kosteniuk, P., Haslett, J., Kendall, D. J., and Wimperis, J. (1985), "WAMDII: wide-angle Michelson Doppler imaging interferometer for Spacelab," *Applied Optics*, 24, 1571–1584.

Shor, P. W. (1994), "Algorithms for quantum computation: Discrete logarithms and factoring," in *Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on*, pp. 124–134, IEEE.

Shor, P. W. and Preskill, J. (2000), "Simple proof of security of the BB84 quantum key distribution protocol," *Physical Review Letters*, 85, 441.

Tatarski, V. (1971), *The Effects of the Turbulent Atmosphere on Wave Propagation*, Jerusalem: Israel Program for Scientific Translations.

Teyssandier, F. and Prêle, D. (2010), "Commercially available capacitors at cryogenic temperatures," in *Ninth International Workshop on Low Temperature Electronics-WOLTE9*.

Tomamichel, M., Lim, C. C. W., Gisin, N., and Renner, R. (2012), "Tight finite-key analysis for quantum cryptography," *Nature Communications*, 3, 634.

Ursin, R., Tiefenbacher, F., Schmitt-Manderbach, T., Weier, H., Scheidl, T., Lindenthal, M., Blauensteiner, B., Jennewein, T., Perdigues, J., Trojek, P., et al. (2007), "Entanglement-based quantum communication over 144 km," *Nature Physics*, 3, 481.

Verevkin, A., Zhang, J., Sobolewski, R., Lipatov, A., Okunev, O., Chulkova, G., Korneev, A., Smirnov, K., Goltsman, G., and Semenov, A. (2002), "Detection efficiency of large-active-area NbN single-photon superconducting detectors in the ultraviolet to near-infrared range," *Applied Physics Letters*, 80, 4687–4689.

Verma, V. B., Horansky, R., Marsili, F., Stern, J. A., Shaw, M. D., Lita, A. E., Mirin, R. P., and Nam, S. W. (2014a), "A four-pixel single-photon pulse-position array fabricated from WSi superconducting nanowire single-photon detectors," *Applied Physics Letters*, 104, 051115.

Verma, V. B., Korzh, B., Bussières, F., Horansky, R. D., Lita, A. E., Marsili, F., Shaw, M. D., Zbinden, H., Mirin, R. P., and Nam, S. W. (2014b), "High-efficiency WSi superconducting nanowire single-photon detectors operating at 2.5 K," *Applied Physics Letters*, 105, 122601.

Verma, V. B., Korzh, B., Bussieres, F., Horansky, R. D., Dyer, S. D., Lita, A. E., Vayshenker, I., Marsili, F., Shaw, M. D., Zbinden, H., Mirin, R. P., and Nam, S. W. (2015), "High-efficiency superconducting nanowire single-photon detectors fabricated from MoSi thin-films," *Optics Express*, 23, 33792.

Wesely, M. L. (1976), "The combined effect of temperature and humidity fluctuations on refractive index," *Journal of Applied Meteorology*, 15, 43–49.

Wiesner, S. (1983), "Conjugate Coding," *SIGACT News*, 15, 78–88.

Wu, J., You, L., Chen, S., Li, H., He, Y., Lv, C., Wang, Z., and Xie, X. (2017), "Improving the timing jitter of a superconducting nanowire single-photon detection system," *Applied Optics*, 56, 2195.

Yang, J. K. W., Kerman, A. J., Dauler, E. A., Anant, V., Rosfjord, K. M., and Berggren, K. K. (2007), "Modeling the electrical and thermal response of superconducting nanowire single-photon detectors," *IEEE Transactions on Applied Superconductivity*, 17, 581.

Zadeh, I. E., Los, J. W., Gourgues, R. B., Steinmetz, V., Bulgarini, G., Dobrovolskiy, S. M., Zwiller, V., and Dorenbos, S. N. (2017), "Single-photon detectors combining high efficiency, high detection rates, and ultra-high timing resolution," *APL Photonics*, 2, 111301.

Zeitler, C., Graham, T., Bernstein, H., Kwiat, P., and Chapman, J. (2016), "Superdense teleportation for space applications," in *SPIE LASE*, pp. 973912–973912, International Society for Optics and Photonics.

Zhao, Q., McCaughan, A. N., Dane, A. E., Najafi, F., Bellei, F., De Fazio, D., Sunter, K. A., Ivry, Y., and Berggren, K. K. (2014), "Eight-fold signal amplification of a superconducting nanowire single-photon detector using a multiple-avalanche architecture," *Optics Express*, 22, 24574.

Biography

Clinton Terry Cahall lived his childhood years in Georgetown, Ohio where he participated in basketball, cross country, track, and is the 2004 Brown County Fair Market Wether Grand Champion. Clinton graduated from Georgetown High School in 2007 and began his undergraduate education at Centre College in Danville, Kentucky. At Centre, Clinton continued to compete in cross country and track, and developed a love for physics.

Clinton earned a B.S. in physics from Centre in 2011 and a year he later moved to London, England to begin his master's degree at Imperial College London. While at Imperial, Clinton was introduced to quantum information science and he did his master's thesis project on a cavity-assisted single-photon source in Prof. Edward Hind's group under the direction of Dr. Jaesuk Hwang. He earned an M.Sc. in physics in 2013 and joined Prof. Jungsang Kim's group in the Electrical and Computer Engineering Department at Duke University in the spring of 2014.

While at Duke, Clinton worked in the MIST lab under Prof. Jungsang Kim and in collaboration with Prof. Daniel Gauthier to develop a single-photon detection system for high-rate, free-space quantum communication. During his time in Durham he did quantum physics, married his wife Bekah, competed in distance running, adopted an American Staffordshire Terrier named Bell, and together with his wife fostered 12 pit-bull rescue dogs to adoption. He completed his Ph.D. in 2019.