Indoor Free-space Quantum Key Distribution In Daylight

Vincent Lee

Wolfson College

Supervisor: **Dominic O'Brien**



Michaelmas Term 2022

A thesis submitted for the Degree of Doctor of Philosophy

Department of Engineering Science

University of Oxford

Parks Road, Oxford OX1 3PJ

I dedicate this thesis to my parents, Tin and Cecilia Lee.

Without your love and support, none of this would be possible.

I am forever grateful to you.

Abstract

Privacy is a major concern in the digital information era. As the Quantum Computer becomes a real possibility, conventional encryption schemes will not suffice to protect user information. One practical method that can ensure privacy and security is Quantum Key Distribution (QKD). QKD is an encryption protocol that uses quantum mechanics and physical properties of light to guarantee security. QKD has been demonstrated for long distance optical communications, terrestrial and free-space, but not in indoor optical wireless environments.

In this work, first, the security concerns of conventional encryption schemes are introduced, and a literature review of quantum communications is undertaken. Second, an indoor QKD system model is evaluated and initial QBER simulations suggest new feasible wavelengths for QKD operation. Wavelengths in 'quiet' regions of the solar spectrum, such as the atmospheric absorption bands, are promising candidates. Third, an experiment and simulation are conducted and analysed which indicate the carbon dioxide and water absorption band (1351 – 1414 nm) is a promising wavelength region for QKD operation for indoor optical wireless environments. The aim is to show the feasibility of the wavelength region around 1370 nm as a necessary step towards a low noise QKD receiver for indoor optical wireless links in a practical environment. Fourth, a static line-of-sight indoor free-space QKD link experiment using BB84 protocol at 1371.5 nm is successfully demonstrated. This experiment was designed and implemented during the COVID-19 pandemic between 2020 – 2022. Two of the four SPAD modules (id221) used in the experimental apparatus were on loan to our group from ID Quantique from March to May 2022. The other two SPAD modules (idQube) were purchased by our Optical Wireless Communications group in Oxford. A series of experiments were conducted to test the robustness of a free-space QKD system operating at 1371.5 nm in the presence of ambient light. The QKD system at 1371.5 nm is robust to ambient light and to the author's knowledge, the

first of its kind. Fifth, the feasibility of using a digital micromirror device (DMD) as a beam steering device at the transmitter is evaluated. Plans to incorporate the DMD into the QKD system are discussed. Finally, conclusions, improvements, and future work are discussed.

Acknowledgments

First and foremost, I would like to thank my supervisor Professor Dominic O'Brien for having the patience to guide and support me through my DPhil. It has been a journey to say the least, especially through the challenging years of COVID-19. I want to thank Grahame Faulkner for his helpful discussions for my experimental designs, troubleshooting issues, and also supporting me through tough times. I want to thank Andy Schreier, Ravinder Singh, Hyunchae Chun, and Weida Zhang for helpful discussions and support in the laboratories.

I want to thank James Farmer, Paramin Sangwongngam, Son Chu, and Akash Trivedi for your continued friendship over the past 6 years. I am grateful to have met you and you've definitely made my Oxford experience a joy.

I want to thank James for being there to bounce ideas off of; your insight has been invaluable and helped make my ideas clearer. Thank you for inviting me to Thanksgiving 2019! It was my first Thanksgiving overseas and it really meant a lot. I can definitely say I was very thankful for the experience.

I want to thank Paramin for also being there to support me in giving me feedback on my ideas. When I first got into the office, you were the first person to approach me to say if I ever needed anything, just ask. Thank you for reaching out and finding the time for me even though you're 7 hours ahead in Thailand!

I want to thank Son for all the fun times at the pub, discussing and playing basketball, and chatting about life in general. It was a welcome break from my studies. I remember when I first

got into the office, and you asked me “Do you watch the NBA?” then I knew we’d be great friends.

I want to thank Akash for being the best flat mate anyone could ask for. We became friends immediately once we connected over our love of food, travel, and Space. Next time you’re in the USA, I will show you the best food, sights, and of course the Space Shuttle Discovery! It’s by my house.

I want to thank my girlfriend Zsofi Jaszberenyi for being so supportive. You’re the best thing that’s happened to me.

I want to thank Zsofi’s mom Krisztina Karasz for keeping me alive during the last edits of this thesis. Homemade Hungarian food fuelled me through my final chapters.

I want to thank my parents, Tin and Cecilia, for their continued love and support from the USA. You never stopped telling me how proud you are of me, and this kept me going these last 6 years. It’s been hard to be away for so long. When I first got my letter of acceptance to Oxford, I told you to look at the paper on the kitchen counter. I waited a few moments and then I heard “That’s my son! That’s my son!” You had no hesitation thinking I can do this, and I knew I wanted to make you and myself proud.

Conferences and Publications

[1] **V. Lee**, A. Shreier, G. Faulkner, and D. O'Brien, "Towards the engineering of a Quantum Key Distribution receiver robust to ambient light" in *2022 SPIE Photonex QComms Conference*, 6 – 8 Dec. 2022, pp. 1-8. https://doi.org/10.1117/12.2645135

[2] **V. Lee** and D. O'Brien, "Indoor Optical Wireless Communications using Quantum Key Distribution at 1370 nm," in *2020 IEEE Photonics Conference (IPC)*, 28 Sept. – 1 Oct. 2020, pp. 1-2. https://doi.org/10.1109/IPC47351.2020.9252396

[3] **V. Lee**, "Secure practical indoor optical wireless communications using QKD," in *QCALL Early-Stage Researchers Conference*, Mondello, Sicily, 2019. Poster.

[4] L. Zhou, D. Lowndes, **V. Lee**, I. Mitra, S. Gopal, J. Rarity, G. Faulkner, and D. O' Brien, "Polarization Calibration Scheme for a Practical Handheld Free Space Quantum Key Distribution Link." in *2019 IEEE Globecom Workshops (GC Wkshps)*, 9 – 13 Dec. 2019, pp. 1-5. https://doi.org/10.1109/GCWkshps45667.2019.9024509

Table of Contents

Chapter 1 Introduction 17
1.1 Need for Security and Privacy 17
1.2 Literature Review of Relevant QKD Protocols 20
1.2.1 Prepare-and-Send QKD Protocols 21
1.2.2 Entanglement QKD Protocols 31
1.2.3 Phase-based QKD Protocols 34
1.3 Long Range Free-space QKD Links 36
1.4 Short Range and Indoor Free-space QKD Links 38
1.5 Motivation and Aims for the Thesis 39
1.6 Summary 40

Chapter 2 Free-space QKD for Indoor Wireless Systems using BB84 41
2.1 BB84 Protocol 41
2.1.1 Quantum Bit Error Rate 41
2.1.2 BB84 Attack Methods 42
2.1.3 Decoy State Protocol 47
2.2 Choice of Wavelength 49
2.3 Indoor System Model for QKD 53
2.3.1 Transmitter 55
2.3.2 Receiver 58
2.3.3 Geometrical Link Loss 66
2.3.4 Link impairments 67
2.4 Initial Verification of a QKD Link Model 73
2.5 QKD Link Simulations 77
2.5.1 QBER Estimation in Artificial Lighting at 658 nm 81
2.5.2 QBER Estimation in Sunlight at 658 nm 84
2.6 Line Of Sight QKD Link Simulation at 761 nm 88
2.6.1 QBER Estimation in Artificial Lighting at 761 nm 90
2.6.2 QBER Estimation in Sunlight at 761 nm 91
2.7 Discussions and Observations 95
2.8 Summary 97

Chapter 3 Solar Measurements and Link Simulation at 1370 nm 99
3.1 The use of 1370 nm in QKD links 99
3.2 Ambient Light Measurements 101
3.2.1 Method 1 – Estimation Using Measured Spectra 104
3.2.2 Method 2 – Estimation Using Angular FOV of Collimator 106
3.2.3 Estimated and Measured Results 107
3.3 QBER Estimation in Sunlight at 1370 nm 110
3.4 Discussions and Observations 113
3.5 Summary 113

Chapter 4 BB84 Free-space Experiment at 1371.5 nm under Ambient Light 115
4.1 Halogen Lamp Calibration 115
4.2 QKD Link Simulations under Halogen Lamp 119
4.3 Experimental Apparatus 122
4.3.1 Transmitter 122
4.3.2 Receiver 130
4.4 Experimental Characterisation of the Transmitter 132
4.4.1 Polarisation Angle Calibration 133
4.4.2 Indistinguishability 135
4.4.3 Mean Photon Number 140
4.4.4 Experimental Characterisation of the Receiver 142
4.5 Experimental Methodology 146
4.5.1 Initialisation 149
4.5.2 Experimental Operation 149

4.5.3 Post-processing....150
4.6 Experimental Performance Results for a QKD Link....153
4.6.1 Extinction Ratio and Crosstalk Matrix Results....153
4.6.2 Experimental Performance Results for 30 Minute Experiment....157
4.6.3 Experimental Performance Results for 60 Minute Experiment....160
4.7 Discussions and Observations....164
4.8 Summary....165

Chapter 5 Digital Micromirror Device as part of the QKD Transmitter....166
5.1 Beam Steering for Indoor Free-space QKD Links....166
5.2 Digital Micromirror Device....168
5.3 QKD Transmitter Requirements....171
5.4 Feasibility Tests for DMD as QKD Transmitter....172
5.4.1 Uniform Illumination Test....172
5.4.2 Constant and Time-Invariant Signal Test....175
5.4.3 Linearity in Pixel Illumination Test....177
5.5 Analysis of Polarisation Bases Reflected off DMD Micromirrors....178
5.6 Pointing, Acquisition, and Tracking System with DMD and Retroreflector....185
5.7 Plan to Incorporate a DMD at the QKD Transmitter....187
5.8 Plan to Incorporate a DMD at the QKD Transmitter with a Pointing, Acquisition, and Tracking System....191
5.8.1 System Architecture....192
5.8.2 Choice of Beam Splitter....194
5.9 Discussions and Observations....195
5.10 Summary....196

Chapter 6 Conclusions and Future Work....197
6.1 System Improvements....201
6.1.1 Degree of Polarisation Experiment (1 week)....201
6.1.2 Visible Light Communications (1 month)....202
6.1.3 Transmitter and Receiver Time Synchronisation for Gating (3 months)....202
6.1.4 DMD Tracking System (3 months)....202
6.1.5 Asynchronous Trigger (3 months)....203
6.2 Future Work....204
6.2.1 Longer Link Distances (1 month)....204
6.2.2 Transmitter and Receiver Alignment (3 months)....204
6.2.3 Smaller Transmitter Form-Factor (3 months)....205
6.2.4 Further Investigation into 1351 – 1414 nm Spectral Region (1 month)....205
6.2.5 RFI QKD Protocol (6 months)....206

References 207

List of Figures

Figure 1: Diagram of the ideal Bennett and Brassard 1984 (BB84) protocol 22
Figure 2: Diagram of Eve and Bob's knowledge of the key during the process from sifted key to secret key 24
Figure 3: Diagram of mutual information between Alice and Bob IA, B and Alice and Eve IA, E vs QBER.....43
Figure 4: System overview of an indoor free-space QKD link in the presence of artificial lighting and sunlight 53
Figure 5: Diagram of an indoor free-space BB84 link 54
Figure 6: Plot of the probability of photon generation vs number of photons per pulse for a WCP source. 56
Figure 7: General BB84 transmitter design.....57
Figure 8: Plots of the detector characteristics for a typical NIR SPAD module. 61
Figure 9: General BB84 receiver design 62
Figure 10: Diagram of spectral filter passband shift and FOV.....65
Figure 11: Plot of spectral filter bandwidth Δ vs half angle field of view of the detector Ψc for two wavelengths in the visible region of the optical spectrum.....66
Figure 12: Plot of normalised relative intensity vs wavelength of one Cree LED bulb.....69
Figure 13: Plot of photons.s $-$ 1.m $-$ 2.sr $-$ 1.nm $-$ 1 vs wavelength of the LED model. ...71
Figure 14: Plots of the ASTM AM1.5 solar standard in log10 scale.....72
Figure 15. Plots of QBER vs total noise count rate per SPAD for the QKD link simulations for the short range QKD link experiments 75
Figure 16: Plots of QBER vs total noise count rate per SPAD for QKD link simulations using parameters from H. Chun et al. 2017.....77
Figure 17: Plots of effective area (left y-axis) and link loss (right y-axis) vs half angle FOV of the entrance pupil for etendue-limited receiver models 79
Figure 18: Plots of the LED model and sunlight spectra in the visible region around 658 nm81
Figure 19: Plot of photons.s $-$ 1.m $-$ 2.sr $-$ 1.nm $-$ 1 vs wavelength for the narrowband filtered spectrum of the LED model centred at 658 nm 82
Figure 20: Plot of QBER vs total noise count rate per SPAD for the QKD link simulations under filtered LED lighting at 658 nm 83
Figure 21: Plot of photons.s $-$ 1.m $-$ 2.sr $-$ 1.nm $-$ 1 vs wavelength for the narrowband filtered sunlight spectrum centred at 658 nm 84
Figure 22: Plot of QBER vs total noise count rate per SPAD for the QKD link simulations under filtered sunlight at 658 nm.....85
Figure 23: Plots of the LED model and sunlight spectra in the visible region around 761 nm89
Figure 24: Plot of photons.s $-$ 1.m $-$ 2.sr $-$ 1.nm $-$ 1 vs wavelength for the zoomed-in narrowband sunlight spectrum around 761 nm 90
Figure 25: Plot of QBER vs total noise count rate per SPAD for the QKD link simulations under filtered LED lighting at 761 nm 91
Figure 26: Plot of photons.s $-$ 1.m $-$ 2.sr $-$ 1.nm $-$ 1 vs wavelength for the narrowband filtered sunlight spectrum centred at 761 nm 92
Figure 27: Plot of QBER vs total noise count rate per SPAD for the QKD link simulations under filtered sunlight at 761 nm.....93
Figure 28: Plots of the ASTM AM1.5 spectrum between 1351 – 1414 nm.....100
Figure 29: Experimental apparatus for ambient light experiment using spectrometer and SPAD module. 101
Figure 30: Plots of the measured ambient light spectra captured by the NIR Flame spectrometer.....103
Figure 31: BB84 receiver design 110

Figure 32: Plot of QBER vs total noise count rate per SPAD for QKD link simulations under filtered sunlight at 1370 nm 111
Figure 33: Plots of the measured ambient light spectra with measured halogen spectrum at 800 lx. 117
Figure 34: Picture of the halogen lamp illuminating the QKD receiver inside the blackout box. 118
Figure 35: Plot of QBER vs total noise count rate per SPAD for QKD link simulations at 41.67 MHz under the halogen lamp at 800 lx. 120
Figure 36: Plot of QBER vs total noise count rate per SPAD for QKD link simulations at 10 MHz under the halogen lamp at 800 lx. 121
Figure 37: Picture of the experimental QKD transmitter apparatus 122
Figure 38: Block diagram of the QKD transmitter assembly. 123
Figure 39: Picture of lasers 124
Figure 40: Picture of temperature controllers 125
Figure 41: Picture of the spatial filter 127
Figure 42: Picture of the optical apparatus of the QKD receiver 130
Figure 43: Block diagrams of the QKD receiver. 131
Figure 44: Picture of the QKD receiver inside blackout box 132
Figure 45: Plot of the measured transmitter pulses in voltage vs time for the four lasers. 138
Figure 46: Plot of the measured spectra in normalised relative intensity vs wavelength for the four lasers. 139
Figure 47: Plot of time of arrivals for one receiver channel. 141
Figure 48: Normalised extinction ratio and crosstalk matrices 144
Figure 49: Experimental system block diagram for BB84 free-space QKD system. 147
Figure 50: Picture of the experimental apparatus 148
Figure 51: Crosstalk matrices for the 30 minute experiment. 154
Figure 52: Crosstalk matrices for the 60 minute experiment. 155
Figure 53: Plot of the results for the 30 minute experiment. 157
Figure 54: Plot of the results for the 60 minute experiment. 161
Figure 55. Indoor free-space QKD link in the presence of artificial lighting and sunlight. 166
Figure 56: DMD optical switching principle. 169
Figure 57: Texas Instruments Lightcrafter 4500 internal layout 170
Figure 58: Experimental setup diagram of Texas Instruments Lightcrafter 4500 projecting a solid red image onto a screen. 173
Figure 59: Plot of the measured waveforms in Volts vs Time at photo detector locations 1 through 6. 174
Figure 60: Plot of the top section of the waveform for location 5 in Volts vs Time. 176
Figure 61: Diagram of the angular position of the DMD and the three states with respect to the QKD transmitter. 179
Figure 62. Plot of reflectance coefficients Rs and Rp for aluminium at 1371.5 nm vs the incident angle 182
Figure 63. Plot of the real refractive index (nR) of the amplitude reflection coefficients rs and rp vs the incident angle 182
Figure 64: Plot of the phase shifts of amplitude reflection coefficients rs and rp vs the incident angle 183
Figure 65: Block diagram of the experimental setup for the PAT system. 186
Figure 66: Picture of a retroreflector illuminated by the Lightcrafter 4500. 187
Figure 67: Block diagram of the planned experimental QKD system with the DMD incorporated into the QKD transmitter. 188
Figure 68: Block diagram of the planned system architecture with the PAT system 192

List of Tables

Table 1: Typical LED light bulb emission parameters 69
Table 2. Short range QKD link simulation parameters. 73
Table 3: QKD link noise and receiver model parameters. 78
Table 4. Parameters for receiver cases 1 and 2 to conserve etendue for geometrical link loss at 14 dB 80
Table 5: Total noise count rate per SPAD for LED lighting filtered at 658 nm 83
Table 6: Total noise count rate per SPAD for sunlight filtered at 658 nm 85
Table 7: Total noise count rate per SPAD for LED lighting filtered at 761 nm 90
Table 8: Total noise count rate per SPAD for sunlight filtered at 761 nm 92
Table 9. Results summary of the QKD link simulations at 658 nm. 95
Table 10. Results summary of the QKD link simulations at 761 nm. 96
Table 11: Estimated and measured photon counts per second for the different ambient light scenarios. 108
Table 12: Results summary of QKD link simulations at 1370 nm. 113
Table 13: QKD link simulation parameters for repetition rates 41.67 MHz and 10 MHz. 119
Table 14: Centre Wavelength Parameters for Lasers. 126
Table 15: Transmittances of the four receiver channels. 132
Table 16: Ideal and measured polarisation angles for each transmitter basis. 134
Table 17: Crosstalk polarisation error calculations for 30 minute experiment 155
Table 18: Crosstalk polarisation error calculations for 60 minute experiment 156
Table 19: Statistical analysis for the 30 minute experiment 158
Table 20: Link budget analysis for 30 minute experiment 159
Table 21: Statistical analysis for the 60 minute experiment 162
Table 22: Link budget analysis for the 60 minute experiment 163
Table 23: Power measurements for the red LED for one to eight pixels. 178
Table 24: Minimum number of pixels for the DMD to create two beam spot sizes 191

Glossary of Acronyms

AC – Alternating current

AES – Advanced encryption standard

AOI – Angle of incidence

APD – Avalanche photo diode

ASTM – American society for testing and materials

ATM – Automated teller machine

B92 – Bennett 1992 protocol

BB84 – Bennett and Brassard 1984 protocol

BBM92 – Bennett Brassard Mermin 1992 protocol

BS – Beam splitter

BSM – Bell state measurement

CAD – Computer aided design

COW-QKD – Coherent one way QKD protocol

CPS – Counts per second

CV-QKD – Continuous variable QKD protocol

CW – Continuous wave

CWDM – Coarse wavelength division multiplexing

CWL – Centre wavelength

D/A – Diagonal/anti-diagonal orthogonal basis pair

DC – Direct current

DFB – Distributed feedback

DLP – Digital light processing technology

DMD – Digital micromirror device

DOF – Degree of freedom

DPS-QKD – Differential phase shift QKD protocol

DV-QKD – Discrete variable QKD protocol

DWDM – Dense wavelength division multiplexing

E91 – Ekert 1991 protocol

ECC – Elliptic Curve Cryptography

FOR – Field of regard

FOV – Field of view

FPGA – Field programmable gate array

FSM – Fast steering mirror

FSO – Free-space optical

FWHM – Full width half maximum

GLLP – Gottesman Lo Lutkenhaus Preskill

He-Ne – Helium neon laser

H/V – Horizontal/vertical orthogonal basis pair

HWP – Half wave plate

IF – Interference filter

IoT – Internet of things

LED – Light emitting diode

LEO – Low earth orbit

LOS – Line of sight

LP – Linear polariser

LTE – Long term evolution

MDI-QKD – Measurement device independent QKD protocol

MEMS – Micro-electromechanical systems

MFD – Mode field diameter

NA – Numerical aperture

NIM – Nuclear instrumentation module

NIR – Near infrared radiation

NIST – National Institute of Standards and Technology

NTC – Negative temperature coefficient

OAM – Orbital angular momentum

OD – Optical density

PAT – Pointing, acquisition, and tracking

PBS – Polarising beam splitter

PDE – Photon detection efficiency

PDF – Probability distribution function

PLOB – Pirandola, Laurenza, Ottaviani, Banchi

PNS – Photon number splitting

PON – Passive optical network

PPS – Photons per second

PSD – Position sensing detector

PSK – Phase-shift Keying

PWM – Pulse width modulation

Q – Quarter wave plate

QBER – Quantum bit error rate

QKD – Quantum key distribution

RFI-QKD – Reference frame independent QKD protocol

RSA – Rivest Shamir Adleman encryption standard

Rx – Receiver

SARG04 – Scarani, Acin, Ribordy, Gisin 2004 protocol

SLM – Spatial light modulator

SMF – Single mode fibre

SNR – Signal to noise ratio

SNSPD – Superconducting nanowire single photon detector

SPAD – Single photon avalanche diode

SSP – Six state protocol

SWaP – Size, weight, and power

TCSPC – Time-correlated single-photon counter

TEC – Thermoelectric cooling

TF-QKD – Twin Field QKD protocol

TIR – Total internal reflection

Tx – Transmitter

UAV – Unmanned aerial vehicle

USB – Universal Serial Bus

VCSEL – Vertical cavity surface emitting laser

VLC – Visible light communications

WCP – Weak Coherent Pulse

WXGA – Wide extended graphics array

XPR – eXpanded Pixel Resolution

Chapter 1 Introduction

In this chapter, the purpose of quantum cryptography and the need for quantum key distribution (QKD) as a method to encrypt and secure optical communications is established. A literature review of relevant QKD protocols such as prepare-and-send, entanglement-based, and phase-based protocols is conducted. A general overview of the BB84 protocol including the procedure and alternatives to the BB84 protocol are described. The challenges of free-space QKD links are then discussed, together with a literature review of long range, short range, and indoor free-space QKD demonstrations. Finally, the motivation for QKD in indoor spaces and aims for the thesis are discussed.

1.1 Need for Security and Privacy

Secure digital communication is essential in the modern environment. Personal computers, laptops, and smart phones enable users to communicate over the Internet, access personal information online, and participate in electronic commerce (e-commerce). In the Internet of Things (IoT [1]) where the Internet and data communications connect billions of devices together, security and privacy are major concerns. Privacy can be defined for communications and information. Privacy of communications is "the protection of the information that is carried through any medium between two parties. This includes email, mail, and telephone. Information privacy refers to personal data that is collected and processed by an organization, such as medical records and credit card information" [2]. All the digital content shared between devices (i.e. passwords, purchase transactions, health records, private messages) should be secured and kept private.

Communications can be intercepted. Two types of digital communications are prevalent in modern society: radio and optical fibre. Cellular communication, such as Long Term Evolution

(LTE), is a radio frequency technology that offers mobile phone service, text messaging service, and mobile Internet access. LTE is more secure than its predecessors, but LTE is still vulnerable to hacking exploits such as call interception and device and identity tracking [3]. Wi-Fi is another radio frequency technology that offers large area Internet coverage and the ability to support Internet access to multiple users at once. However, Wi-Fi is susceptible to hacking from software tools designed to exploit passwords and Wi-Fi router features [4].

Telecommunications companies rely on optical fibre networks to offer customers broadband high speed Internet directly to their homes (fibre to the home [5]). However, optical fibres can be tapped with tools that clamp onto the fibre and this tap feeds the information from the fibre to a computer. This was demonstrated in [6], such that a hacker can read all the unsecure information coming across the fibre.

The fundamental tool in preserving the privacy of communications and information is digital encryption. Encryption is a scheme to ensure the privacy of messages between two parties in the presence of an eavesdropper. The transmitter (Alice) uses a key to convert the message (plaintext) into an unintelligible message (ciphertext). She sends the ciphertext to the receiver (Bob) and only Bob knows the key to decrypt the ciphertext to reveal the plaintext. Without knowledge of the key, the eavesdropper (Eve) will only see the ciphertext [7].

There are two types of encryption: symmetric and asymmetric. Symmetric encryption, also known as private key encryption, uses the same key for encryption and decryption. Alice must tell Bob the private key without Eve knowing. Consequently, if Eve knows the key, she can decrypt the ciphertext and read all of the plaintext message contents [8]. At present, the Advanced Encryption Standard (AES) is the preferred symmetric encryption scheme because of its strength against brute force attacks [9]. AES encodes 128 bit blocks of a message using

key lengths of 128, 192, and 256 bits [10]. The minimum 128-bit key length encryption requires an extremely long length of time to break [11]. The use of AES is widespread from encryption on smart phones and encrypted messaging apps to Internet security (e.g. Wi-Fi networks, websites, cloud storage, Virtual Private Network service).

Symmetric key ciphers are not vulnerable to quantum attacks. At present, a brute force attack such as Grover's quantum search algorithm [12] is considered the optimum attack method for the symmetric key cipher AES. The speedup this offers compared with classical methods is quadratic and a small increase in key length is sufficient to ensure security.

Asymmetric encryption, also known as public key encryption, uses two keys: one public and one private. The public key can be used by everyone to encrypt information. The private key is used to decrypt the ciphertext created by the public key. The advantage of asymmetric encryption is users only have to safeguard the private key and this private key is not shared across the Internet to another party [8]. Currently, the preferred asymmetric encryption scheme is RSA named after the inventors Rivest, Shamir, Adleman [13]. The encryption is based on the factorisation of composite numbers into two 100 – 200 bit prime factors. Similar to AES, RSA is usually considered safe because an adversary could take an extremely long length of time to crack the key through brute force [14]. Another major form of asymmetric encryption is elliptic curve cryptography (ECC) [15, 16]. ECC uses the algebraic difficulty in solving a discrete logarithm for a random component of the elliptic curve when an initial base point is used for the public key. The size and complexity of the ECC keys depend on the discrete number of integer pairs that satisfy the equation $y^2 = x^3 + ax + b$. ECC offers increased computational complexity with smaller key lengths compared to RSA.

Existing encryption schemes depend on the computational complexity of the attacks on the protocol and an adversary's lack of computer resources and time. An algorithm for cracking RSA and ECC encryption, Shor's Algorithm [17], exists but needs a Quantum Computer. As the Quantum Computer becomes a real possibility, the computer can theoretically crack public key cryptosystems exponentially faster than conventional computers [18]. Benchmark simulations of large-scale fault-tolerant quantum attacks on AES, RSA, and ECC encryption schemes are found in [19] and these evaluate the number of physical qubits, gates, surface code cycles, and time necessary for the quantum attacks. Long term security is therefore a major concern and conventional encryption schemes will not suffice to protect user information. Work on 'post-quantum' cryptography is also beginning to address the long term security concern [20, 21].

In this work we focus on secure communications techniques that ensure the adversary does not have information about the generated key. The shared secret key can then be used in AES or similar symmetric encryption schemes, removing the weakness of asymmetric key sharing.

1.2 Literature Review of Relevant QKD Protocols

Quantum communications offers the potential for secure communications by using Quantum Mechanics and the physical properties of light to guarantee security. Quantum Mechanics guarantees security based on two principles: the Heisenberg Uncertainty Principle and the No Cloning Theorem. The Heisenberg Uncertainty Principle [22, 23] states that the physical properties of a particle (i.e. position and momentum) cannot be precisely measured simultaneously. In other words, one physical property of a quantum system can be measured with certainty; however the conjugate physical property cannot be measured with certainty. Developing on this idea, the No Cloning Theorem [24] states that if Eve were to intercept a photon from Alice, Eve cannot recreate the exact same photon and send it to Bob. One practical

method that can ensure privacy and security is Quantum Key Distribution (QKD). QKD is a method to create a secret shared digital encryption key between two parties, Alice and Bob, in the presence of Eve. QKD allows the secure distribution of encryption keys and offers enhanced physical layer security with eavesdropper detection to guarantee security. The next sections describe the relevant QKD protocols in the current research such as prepare-and-send QKD protocols, entanglement QKD protocols, and phase-based QKD protocols.

1.2.1 Prepare-and-Send QKD Protocols

There are two main categories of non-entanglement QKD protocols: Discrete Variable QKD (DV-QKD) and Continuous Variable QKD (CV-QKD). The difference between DV-QKD and CV-QKD is the degrees of freedom used to encode quantum information. Consequently, each category of protocol has a different type of detection. DV-QKD encodes quantum information in a finite-dimensional state space (e.g. single photons) and uses a photon counting method that utilises single photon detectors to register a count when a photon arrives at the detector. The number of measurement outcomes are a count or no count. CV-QKD encodes quantum information in infinite-dimensional state space (e.g. Gaussian states [25] on the amplitude and phase of the quantised electromagnetic field of the pulses) and uses the homodyne or heterodyne detection method. This uses an interferometer and local oscillator to evaluate the received signal state's quadrature components. The measurement outcomes for the quadrature components are a continuous range.

1.2.1.1 BB84 Protocol

In 1984, Charles H. Bennett and Gilles Brassard created the first theoretical QKD protocol [26]. The BB84 protocol is a DV-QKD protocol that uses polarisation conjugate pairs

horizontal/vertical and diagonal/anti-diagonal as its bases to create a secret shared digital encryption key. Figure 1 illustrates the operation of the ideal BB84 protocol.

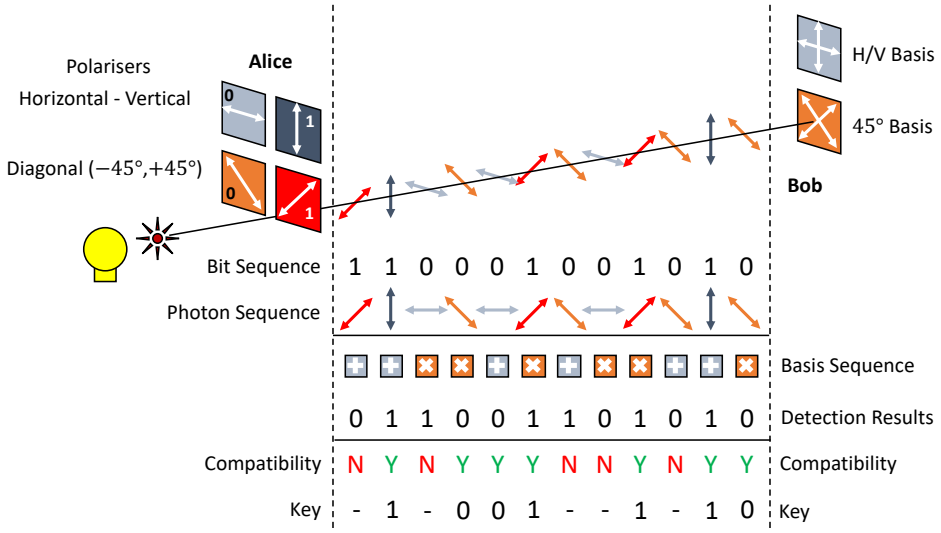


Figure 1: Diagram of the ideal Bennett and Brassard 1984 (BB84) protocol [27]. The overall diagram shows Alice with a single photon source and four linear polarisers (left), the quantum channel (middle), and Bob with two polarisation conjugate pairs of bases (right). Bob uses four detectors and groups two detectors for H/V basis measurement and the remaining two detectors for D/A basis measurement. The top block shows the photons sent by Alice (Photon Sequence) and the corresponding bit values (Bit Sequence). The middle block shows the bases choices made by Bob (Basis Sequence) and the corresponding bit values (Detection Results). The bottom block shows the compatibility of the photons sent by Alice with the bases choices made by Bob. The photons measured with compatible bases have correct detection results. Only these results are kept and make up the shared sifted quantum key for Alice and Bob to use. It should be noted that the detection result is random (0 and 1 have equal probability) when a photon and a basis are incompatible.

1.2.1.2 BB84 Procedure

1) Alice and Bob establish a public (classical) channel to authenticate each other. The biggest assumption in QKD is correct authentication on a public channel (for instance, Alice confirms she's Alice and Bob confirms he's Bob). Failure to do so could result in

a man in the middle attack where Eve impersonates Bob and Alice sends all her photons to Eve. However, a way to improve authentication by classical means is a shared secret [28] between Alice and Bob. It is also assumed the public channel cannot be jammed to interfere with the communication between Alice and Bob.

2) Alice makes a random choice to encode photons using H, V, D, or A polarisers and sends the polarised photons to Bob.
3) Bob makes a random choice to measure each photon using either H/V or D/A basis. Bob has a total of four detectors. He uses two detectors for H/V basis measurement and an additional two detectors for D/A basis measurement.
4) On the public channel, Bob verifies with Alice which basis (H/V or D/A) he used to measure each photon.
5) Alice tells Bob which basis to keep and, through this process of sharing and confirming basis measurements, Alice and Bob now have the same sifted key without publicly revealing the key. The maximum length of the sifted key is 50% of the qubits sent by Alice due to the equal probability of Bob measuring with two bases: H/V and D/A. In other words, 50% of the qubits are discarded because Bob's measurement results in the conjugate basis are random and ambiguous.

Figure 2 shows the steps from a sifted key to a secret key and how much knowledge Eve gains in each step. Ideally, the process ends at step 5 where Alice and Bob have a shared sifted key. However, in practice, errors enter the process due to the use of non-ideal sources and false positive readings when Bob measures photons. It is assumed that all errors are caused by Eve using attack methods and she has gained some knowledge of the key (Figure 2a). Alice and Bob can check for Eve's interception using the Quantum Bit Error Rate (QBER). This is the error rate in the conjugate basis compared to the key generation basis which indicates possible information gain to Eve through eavesdropping. The QBER is calculated as a ratio of the total

number of errors to the total number of received photons and displayed as a percentage [29]. Each QKD protocol has a QBER threshold. This threshold indicates the maximum acceptable error at the point where Bob knows more than Eve. Any QBER above the threshold indicates that there is a risk that Eve might know more than Bob. Hence, Eve might know the key. A common threshold for the QBER in the BB84 protocol is 11% [30-32].

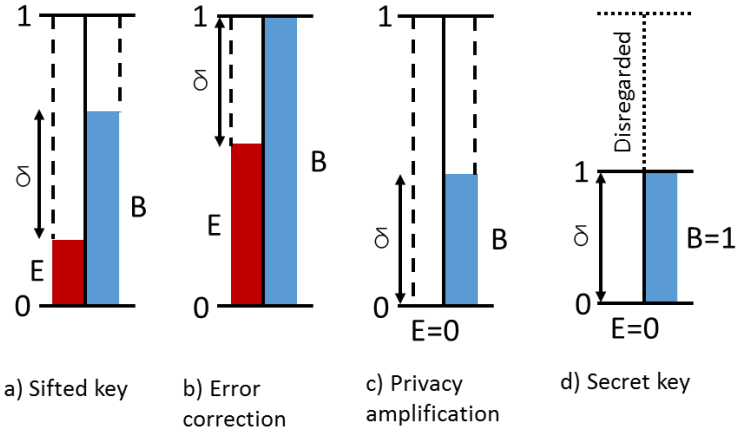


Figure 2: Diagram of Eve and Bob's knowledge of the key during the process from sifted key to secret key [29]. (a) The sifted key step shows the amount of information gained by Eve (E) through eavesdropping relative to Bob's (B) knowledge of the key. δ is the difference between Bob and Eve's knowledge of the key. (b) The error correction step allows Bob to obtain the full key and also increases the information gained by Eve. (In practice, the error correction codes can reveal more information than strictly required to correct for errors. This enables Eve to gain more information.) (c) The privacy amplification step shows Eve's knowledge of the key reduces to zero. (d) The secret key step shows Bob has full knowledge of the new shorter key.

If the QBER is below the threshold, Alice and Bob can continue to create the encryption key. There are two additional steps that ensure a secret key (Figure 2d).

6) Error correction (Figure 2b), also known as reconciliation, is a block-by-block comparison of bits in the sifted key (done recursively) to make sure, in the end, Alice and Bob have high probability of the same sifted key. Alice computes parity bits of

randomly sampled blocks and reveals these to Bob over the public channel, at the expense of Eve learning more information and gaining knowledge about the key. A commonly used type of reconciliation is the Cascade protocol [31] because it is simplest to implement. However, it requires a certain number of iterative exchanges (depending on channel estimated error) between Alice and Bob for block-by-block parity bit comparison.

7) Privacy amplification (Figure 2c) is when, over a public channel, Alice and Bob choose to create a new shorter key from their reconciled key (step 7) by using a hash function. This hash function eliminates Eve's knowledge of the shared key because Eve would need to use brute force of all possibilities to recreate this key from the hash function with her limited knowledge of Alice and Bob's shared key. Cryptographic hash functions are mathematical algorithms (usually one-way, irreversible functions) that accept inputs of arbitrary length and all outputs are of equal length [33]. In QKD, the purpose of a hash function is to increase entropy (uncertainty in the knowledge of the shared key) for Eve.

Therefore, the key generation process has a dual purpose: 1) the key can be used to encrypt the message and 2) to detect Eve and allow Alice and Bob to use or discard the key. The BB84 protocol was proven unconditionally secure in the asymptotic limit (i.e. one-time pad) by Dominic Mayers [34, 35] and further simplified by Peter Shor and John Preskill [30]. The security proof of BB84 was extended to imperfect devices in the asymptotic limit by Daniel Gottesman, Hoi-Kwong Lo, Norbert Lutkenhaus, and John Preskill (GLLP) [36].

Comprehensive analyses of recent advancements in practical QKD systems with realistic devices can be found in [37, 38]. Based on the current technology, a contemporary perspective

on QKD shows two issues in practical QKD systems: imperfect devices and statistical fluctuations in the key length. Imperfect devices such as weak coherent pulse (WCP) sources and detectors are susceptible to side channel attacks by Eve. An example of a WCP source is an attenuated LED or laser that may generate two or more photons per pulse in accordance with the Poisson distribution. A side channel attack or quantum hacking is a method for Eve to gain information about the key from the physical hardware of the transmitter and receiver. For example, if Alice uses a semiconductor laser source for each basis, Eve can potentially analyse the pump-current of each laser source and the times when each laser emitted a pulse. She can find the average time for each pulse to estimate which basis Alice chose. Another example is that the single photon detector at Bob's receiver is not 100% efficient. The detector circuitry may be more sensitive and have higher efficiency to a photon based on the time of arrival. Eve can potentially control and manipulate the timings of the photon detections. Eve can delay the pulses sent by Alice such that Bob will detect the photons and Eve can analyse how the detector responds based on the time of arrival. These are two examples of the device imperfections that allow Eve to potentially hide her presence, manipulate the quantum channel, and enhance her eavesdropping strategies to gain more information about the key.

Furthermore, in the ideal scenario Alice and Bob can perform quantum key exchange indefinitely until they can create an encryption key known as the one-time pad. This is a sufficiently long key that is at least equal to the length of the message that Alice tries to send to Bob. However, the quantum transmission between Alice and Bob cannot be infinite, resulting in finite length keys much shorter than the one-time pad. Although shorter key lengths are more susceptible to statistical fluctuations, the effect of the finite block size is to reduce the ratio of the final key to the raw key (i.e. finite key rate is lower than the asymptotic rate) while maintaining a constant final error rate. This ensures the security of the finite key.

1.2.1.3 Efficient BB84 protocol

The BB84 protocol is a symmetric protocol due to the equal probability of Alice sending qubits from her two bases and equal probability of Bob performing measurements using his two bases. This is not efficient because at least half of the qubits sent by Alice are discarded due to mismatches in Bob's choice of basis and the computation of a single bit error rate (QBER) on the entire sifted key.

An efficient BB84 protocol [39] was created by Hoi-Kwong Lo, H. F. Chau, and M. Ardehali in 2005. In this asymmetric protocol, one of the conjugate bases is biased significantly more than the other. The basis distribution is not uniform, such that the bias may be 20% H/V to 80% D/A, for example. The more biased basis is used for key generation and the error rate in this basis is used to calculate the QBER. This affects the error correction information leakage. The error rate of the less biased basis is used to estimate the information gained by Eve from eavesdropping. All of the bits in the less biased basis are revealed and none of the bits in the key generation basis are revealed. This is contrary to the standard BB84 protocol where a random fraction of bits in both bases are publicly revealed. The efficient BB84 protocol was proven to have unconditional security, the same QBER = 11% threshold as the standard BB84 protocol[1], and the basis sifting efficiency approached 100% in the asymptotic limit (i.e. less qubits were discarded in the key generation basis). In this thesis, the standard BB84 protocol is used, not the efficient BB84 protocol. The QBER is used as a single metric for the entire key and the bit error rates are not separated for each individual basis.

[1] In the efficient BB84 protocol, Alice and Bob can accept the security of the quantum transmission for a QBER higher than 11% only if the error rate in the less biased basis is lower to compensate.

1.2.1.4 BB84 Protocol Alternatives

There are alternatives to BB84, including the B92, Six State, and SARG04 protocols, and each have trade-offs. The B92 protocol [40-42] was invented by Charles Bennett in 1992. B92 is a simplified version of BB84 such that only two polarisation states are used. Alice makes a random choice of either H (0˚) or D (45˚) polarisation to encode her qubits and sends a sequence over to Bob. The H (0˚) choice is set as the logical 0 and the D (45˚) choice is set as the logical 1. Bob makes a random choice to measure each photon with either a rectilinear or diagonal basis, similar to BB84. Over the public channel, Bob tells Alice which measured qubits resulted in an outcome of V (90˚) or A (–45˚). These qubits are kept for the sifted key and the remaining qubits are discarded. By measuring the orthogonal polarisation of the incoming photon, Bob is certain that his measurement outcomes are consistent with Alice. The advantage of this protocol over BB84 is Alice and Bob do not need to perform basis reconciliation. This simplifies the protocol and reduces Eve's knowledge of the key. However, the B92 protocol has two disadvantages compared to BB84. B92 offers a slower transmission rate for the raw key compared to BB84 due to fewer polarisation choices, leading to a transmission rate half that of BB84. B92 is also more susceptible to intercept and resend attacks compared to BB84 as Eve knows there are only two polarisation choices.

The Six State Protocol (SSP) [43, 44] was invented by Dagmar Bruß in 1998. SSP is similar to BB84 with the addition of a left and right circular polarisation basis. Alice makes a random choice of one of six polarisations to encode her qubits and sends a sequence over to Bob. Bob measures qubits using one of three possible basis choices which results in this protocol being less efficient than BB84. Theoretically, Alice and Bob can receive a maximum sifted key at 1/3 of the raw key. However, SSP has two advantages over BB84. Eve may be detected more easily since Eve also has 1/3 probability of deciphering each qubit, and the QBER threshold of SSP is 12.6% which is larger than the BB84 threshold [45].

The SARG04 protocol [46, 47] was invented in 2004 by Valerio Scarani, Antonio Acin, Gregoire Ribordy, and Nicolas Gisin. SARG04 is similar to BB84 except in the classical post-processing step for basis reconciliation. Alice makes a random choice between H, V, D, A polarisations to encode her qubits and sends a sequence over to Bob. After Bob has measured all of the qubits, Alice reveals a pair of non-orthogonal basis choices for each qubit she sent. Bob uses this information to infer which polarisation basis is correct for his measurement outcomes. Alice and Bob use the matching qubits to create the sifted key. If Bob is unsure of any of his measurements, these unmatching qubits are discarded. The SARG04 protocol has the advantage of mitigating Photon Number Splitting (PNS) attacks. Practical QKD systems use WCP sources such as lasers and LEDs due to a lack of single photon sources. Lasers and LEDs may send multiple photons in a single pulse, and this is susceptible to Eve keeping one of the photons and going undetected. With the SARG04 protocol, Alice never reveals her basis choices during the basis reconciliation step. Therefore, Eve needs to eavesdrop more to gain more information, and this will lead to her exposure due to the increased QBER. However, the disadvantage is the SARG04 protocol is less efficient than BB84. Theoretically, the maximum sifted key is only 25% of the raw key compared to 50% in the BB84 protocol.

All of these protocols have a reference frame requirement to establish the correct orientation for the H/V and D/A bases. That is, Alice and Bob agree on a common plane of reference where Alice can send her qubits and Bob can measure the qubits in the same orientation to correctly decipher which qubits Alice sent.

1.2.1.5 Reference Frame Independent QKD (RFI-QKD) Protocol

Another DV-QKD protocol is the Reference Frame Independent QKD (RFI-QKD) protocol [48] that was invented by Anthony Laing, Valerio Scarani, John G. Rarity, and Jeremy L.

O'Brien in 2010. The RFI-QKD protocol was proposed for free-space links for ground station-to-LEO satellite communications. RFI-QKD uses six polarisation basis: Left/Right circular polarisations are used for the secret key rate and Horizontal/Vertical and Diagonal/Anti-diagonal polarisations are used for the link security. This protocol assumes the Horizontal/Vertical and Diagonal/Anti-diagonal basis are slowly varying reference frames i.e. satellite rotation with respect to the ground station. RFI-QKD expands on the security of BB84 and relaxes the reference frame requirement [49]. Surface-to-satellite experiments demonstrated the robustness of circular polarisations to atmospheric turbulence [50-53], and research is ongoing to use RFI-QKD for satellite QKD [54]. At present, only short range (less than 1m) free-space links with handheld devices were demonstrated with RFI-QKD [55, 56].

1.2.1.6 Continuous Variable QKD (CV-QKD) Protocol

Continuous Variable QKD (CV-QKD) is a protocol that modulates the amplitude and phase of Gaussian beams to produce the signal states [57-59]. CV-QKD is primarily used in fibre [38, 60-63] due to the fixed attenuation in the fibre channel and the compatibility of the protocol with standard telecommunications components. CV-QKD offers increased key rates compared to DV-QKD protocols due to link loss in the fibre channel. However, CV-QKD is not yet used for free-space communications due to atmospheric turbulence. This causes beam wander and fading which affect the quadrature components of the signal state. Although research is ongoing into mitigating turbulence [64, 65], research has only been investigated for surface-to-satellite communications [66, 67]. In satellite QKD, the downlink (satellite-to-surface) is much preferred over the uplink. The uplink experiences atmospheric turbulence early in the trajectory and this leads to large deviations in the path (also known as the Shower Curtain Effect). There can be 20 dB or greater link loss for the uplink compared to the downlink [68, 69].

1.2.2 Entanglement QKD Protocols

In 2022 Alain Aspect, John F. Clauser, and Anton Zeilinger were awarded the Nobel Prize in Physics for their significant contributions to the field of Quantum Information Science. Their work on quantum entanglement, quantum teleportation or what Albert Einstein called 'spooky action at a distance' helped pave the way for quantum computers, quantum networks, and secure quantum encrypted communication in the modern era [70]. Quantum entanglement is when two particles behave as a single unit and any measurement on one of the particles immediately affects the other particle. Each particle, i.e. an electron, has a wavefunction which is a superposition of two states: spin-up and spin-down. The state of the electron is determined when one electron is measured, for example in the spin-up state. Consequently, the other electron is immediately affected, and the measurement outcome is either the spin-up or spin-down state. For the purposes of entanglement QKD protocols, the entangled state of the particles is typically anti-correlated such that when Alice measures her qubit with an outcome of spin-up, then Bob will measure his qubit with an outcome of spin-down, and vice-versa. This phenomenon is an inherent property of entangled particles. No information is transferred between the particles. The effect can be observed at arbitrarily long distances between the particles.

1.2.2.1 Ekert 1991 (E91) Protocol

The first entanglement QKD protocol was invented by Artur Ekert in 1991 [71]. In the E91 protocol, one entangled-polarisation source sends entangled photon pairs to Alice and Bob. The photon pairs are chosen from a set of four maximally entangled quantum states known as Bell states. Alice and Bob each receive one entangled photon and perform an independent projective local measurement on their entangled photon. Alice and Bob measure the photons by randomly

choosing one of their three polarisation basis choices: Alice uses 0˚, 45˚, 90˚ and Bob uses 45˚, 90˚, 135˚. The basis choices that Alice and Bob have in common (45˚ and 90˚) are used for the quantum key. The measurement outcomes of these two basis choices are anti-correlated (assuming a singlet state) such that when Alice measures one entangled photon, the value of Bob's entangled photon will be the opposite. After confirming they both used the same bases, in order for Bob to get the same sifted key as Alice, he will flip all of outcomes from his measured qubits.

The other qubits that were compared without the same basis choice are used in Bell's inequality [72, 73] for link security to check for eavesdropping. Bell's inequality is a method to verify the entanglement between two particles by applying a constraint on how correlated the measurement outcomes are between two entangled particles. Eq. (1) shows Bell's inequality in the form used for experiments. This is called the CHSH inequality named after its authors John Clauser, Michael Horne, Abner Shimony, and Richard Holt [74].

$$| S | \leq 2, \qquad S = E(a, b) - E(a, b') + E(a', b) + E(a', b') \tag{1}$$

In Eq. (1) S is the figure of merit for the quality of the entangled state, $E(a, b)$ is the expectation value between Alice and Bob's measurement outcomes ($E(a, b)$ is also known as the correlation coefficient), a and a' are the outcomes of Alice's measurements, b and b' are the outcomes of Bob's measurements.

Entanglement violates the CHSH inequality with parameter $| S | = 2\sqrt{2}$. Assuming locality and realism [75, 76], Eq. (1) has a maximum value of $| S | = 2$ for all of the possible combinations of $E(a, b)$. Alice and Bob can set a security parameter of the quantum channel such that parameter $| S | = 2\sqrt{2}$ if the entangled states are undisturbed. Alice and Bob can be certain their entangled qubits are highly correlated and have not been eavesdropped [77-80]. Free-

space QKD experiments were demonstrated using the E91 protocol [81] and modified versions of the E91 protocol [82-84].

1.2.2.2 Bennett Brassard Mermin 1992 (BBM92) Protocol

The BBM92 protocol [85] was invented by Charles Bennett, Gilles Brassard, and N. David Mermin in 1992. BBM92 is an entanglement version of the BB84 protocol. One entangled-polarisation source sends entangled photon pairs to Alice and Bob. Alice and Bob randomly select bases of Horizontal/Vertical (H/V) or Diagonal/Anti-diagonal (D/A) to perform measurements on the photons. Alice and Bob compare over the public channel which bases they used. For the sifted key, Bob will need to flip his qubits as they are anti-correlated with Alice's qubits. Alice and Bob then follow similar steps in the BB84 protocol to check for eavesdropping, apply error correction, and apply privacy amplification. Currently, BBM92 is the entanglement-based protocol that has been used in satellite QKD experiments [86-90].

1.2.2.3 Measurement Device Independent QKD (MDI-QKD) Protocol

The Measurement Device Independent QKD (MDI-QKD) protocol [91] was invented by Hoi-Kwong Lo, Marcos Curty, and Bing Qi in 2012. Entanglement is not explicitly used in MDI-QKD; however MDI-QKD can be considered a time-reversed version of the BBM92 protocol. In MDI-QKD, there is an untrusted node Charlie (or Eve) in between Alice and Bob. Alice and Bob prepare their product states, choose polarisations H, V, D, A at random, and send their qubits to Charlie. Charlie has an apparatus consisting of a 50:50 beam splitter, two polarising beam splitters, and four detectors to perform a Bell State Measurement (BSM). The BSM is a joint measurement on the product states and the measurement outcome corresponds to one of four maximally entangled quantum states known as Bell states. If Alice and Bob sent the same

polarisation, the outcome of a BSM shows a high correlation of the qubits.[2] As part of the protocol, the results of the Bell measurements performed at Charlie are publicly announced to Alice and Bob. Alice and Bob choose the qubits where there are successful BSM outcomes to establish their quantum key. The security of MDI-QKD is assumed because if Charlie (or Eve) attempt to eavesdrop on the Bell measurements, the quantum correlations are destroyed, and Alice and Bob know which qubits are tampered with. Otherwise, if Charlie (or Eve) faithfully announce the results of the Bell measurements, Charlie (or Eve) do not gain any information about the key [38, 92-94]. The advantages of MDI-QKD are that MDI-QKD eliminates the need for a trustworthy measurement device, theoretically eliminates all side channel attacks, and reduces the hardware costs for Alice and Bob down to a low-cost transmitter. Although the protocol is robust to side channel attacks, in practice Alice and Bob should take care to close the side channels and implement a decoy state protocol with MDI-QKD [94]. The receiver apparatus at Charlie (or Eve) can be placed as a node in a network relay [92]. MDI-QKD is primarily used in fibre and not yet in free-space QKD links. However, research is ongoing to use MDI-QKD with a satellite as the untrusted node [95].

1.2.3 Phase-based QKD Protocols

1.2.3.1 Differential Phase Shift QKD (DPS-QKD) Protocol

The Differential Phase Shift QKD (DPS-QKD) protocol [96-98] was invented by Kyo Inoue, Edo Waks, and Yoshihisha Yamamoto in 2002. Alice sends Bob a pulse train of weak coherent pulses. Each pulse is randomly phase modulated by 0 or π. Bob measures each pulse with a one pulse delay Mach-Zehnder interferometer with two detectors: one detector for phase = 0 and the other detector for phase = π. Each adjacent pulse is measured for the phase difference at the

[2] The BSM is different from the measurement of a Bell state. The latter is when Alice and Bob each receive one entangled photon and perform an independent projective local measurement on their entangled photon.

interferometer. A phase = 0 is assigned to logical bit '0' and phase = π is assigned to logical bit '1'. Bob records the time and which detector counts to get a sifted key. Afterwards, Bob tells Alice over the public channel which time bins he recorded for each successful measurement. As Alice knows the times when she sent which pulse, she can create the same sifted key. DPS-QKD is primarily used in fibre and not yet in free-space QKD links.

1.2.3.2 Coherent One-Way QKD (COW-QKD) Protocol

The Coherent One-Way QKD (COW-QKD) protocol [60, 99-102] was invented by Damien Stucki, Nicolas Brunner, Nicolas Gisin, Valerio Scarani, and Hugo Zbinden in 2005. COW-QKD is a type of differential phase shift QKD protocol that uses time bins at the receiver to establish a key. Alice and Bob establish a time of arrival for the time bins. Alice sends a sequence of pulses with a combination of vacuum and non-empty pulses with mean photon number μ, i.e. (0, μ) for logical zero, (μ, 0) for logical one, or (μ, μ) for a decoy state. A 90:10 fibre splitter is used at the receiver in which 90% of the pulses are sent to Bob and 10% of the pulses are sent to a monitor channel to detect an eavesdropper. Bob measures the pulses at his detector and looks in each time bin for the location of the non-empty pulse to determine what value was sent. Bob monitors the pulses with an interferometer in the monitor channel. The security depends on the coherence of successive non-empty pulses in the time bins for example, decoy state (μ, μ) pulses or logical one followed by logical zero, i.e. (0, μ) (μ, 0) pulses. The first COW-QKD free-space link was demonstrated by O. Alia, et. al [103].

After an overview of the relevant QKD protocols, the next two sections describe the current research for long range, short range, and indoor free-space QKD link experiments.

1.3 Long Range Free-space QKD Links

The first BB84 proof of concept experiment was demonstrated in free-space over 32 cm [104]. The experiment was performed in a laboratory and consisted of one LED sending pulses with $\mu = 0.34$ and two photomultipliers with PDE = 9%. The experimental results showed that quantum cryptography was possible and a free-space QKD link was feasible. Thereafter, free-space QKD experiments have been demonstrated for non-entanglement protocols [50, 55, 56, 95, 103-149] and entanglement protocols [81-84, 87-90, 122, 123, 150-154]. The BB84 protocol is used in most free-space QKD links [104, 105, 107, 108, 114, 116, 118, 119, 121, 122, 128-134, 136-138, 140-149].

The current focus in research and development for free-space QKD links is long range communications to facilitate the global quantum network and the quantum internet. Long range free-space QKD links consist of building-to-building communication in urban environments and surface-to-airborne targets. These targets include Unmanned Aerial Vehicles (UAVs), aeroplanes, hot air balloons, and Low Earth Orbit (LEO) satellites. QKD can secure local networks for government buildings and businesses in urban environments. Experiments for free-space QKD between buildings were reported in [119-121, 150]. Cities such as Boston, USA [122], Vienna, Austria [123], and Geneva, Switzerland [155] have deployed operational free-space and fibre QKD links in their metropolitan networks.

Free-space QKD links with UAVs or ‘drones’ can offer a secure quantum network in remote locations. Experiments were demonstrated for surface-to-drone links [148, 149], and links that involved an aeroplane [128] and hot air balloon [129] were demonstrated as feasibility tests for

surface-to-satellite QKD. The use of satellites offers the potential for global coverage with QKD. Satellite QKD experiments utilised microsatellites [50-53] in Low Earth Orbit (LEO) to communicate with ground stations. LEO missions using CubeSats [68, 156-158] were proposed and an experiment was performed on a CubeSat in LEO orbit [159], as well as demonstrations showing the feasibility of satellite QKD [50-53, 107, 130, 131, 151-153, 159-167].

Free-space QKD systems, more specifically satellite QKD, are typically operated in the near infrared regions of the solar spectrum between 800 – 850 nm [83, 86-89, 107, 119, 120, 122, 123, 130, 139, 151, 158, 160]. This is due to an atmospheric transmission window between 780 – 850 nm where the atmospheric scattering has minimal attenuation i.e. 0.1 dB/km in clear weather [60]. More recently, free-space QKD experiments have been demonstrated at 1550 nm [108, 136, 137, 149] in an effort to utilise the same telecommunications wavelength as that used in existing fibre networks. Satellite QKD can potentially operate at 1550 nm due to the atmospheric transmission window around 1550 nm being slightly better than that of 780 – 850 nm, together with a much lower solar irradiance than 780 – 850 nm [108].

There are several challenges in free-space QKD links. The first challenge is the preservation of the qubit state through the atmosphere. Free-space QKD systems primarily implemented the BB84 protocol with polarisation bases. The BB84 protocol can use any two-dimensional quantum degrees of freedom; however the polarisation of a qubit can be preserved through atmospheric turbulence [50-53, 60, 160, 163]. The second challenge is a typical free-space QKD link is fixed or has limited range of movement to ensure line of sight (LOS) communications. Free-space links require a pointing, acquisition, and tracking (PAT) system that establishes and maintains the LOS communications. Free-space link experiments with PAT systems were reported in [168-178]. The third challenge is the free-space QKD system is susceptible to interference and induced noise at the QKD detector from exposure to ambient

light, in particular sunlight. Most free-space QKD links have been demonstrated at night [81-83, 88, 89, 95, 107, 109-111, 119, 121, 128-131, 140, 150-154, 165], in order to reduce the effect of ambient light on the QKD detector. Sunlight is a major challenge for free-space QKD links due to its broad spectrum, and a smaller number of free-space QKD links have been demonstrated during daylight [84, 87, 108, 112-118, 120, 136, 137, 149]. Such links require spectral filtering, a narrow field of view and a small receiver collection area to mitigate the noise from ambient light. For these reasons most free-space QKD links have an extremely narrow FOV, e.g. microradians [81-84, 87, 88, 108, 116, 119, 120, 128, 129, 131, 136, 137, 153, 165], and use pinholes [81, 83, 87, 116, 118, 119, 140, 150, 151, 153] to spatially filter out interference and noise on the QKD detector. In addition, the passband filters used in free-space QKD links have optical bandwidths of 5 nm or less [81-84, 89, 108, 112-114, 117, 118, 129, 131, 151, 153].

1.4 Short Range and Indoor Free-space QKD Links

The majority of the free-space QKD link experiments have been outdoors using the BB84 protocol. Although entanglement protocols have been demonstrated for some systems [81-84, 87, 88, 150-152, 165] these are complex, and BB84 is the most widely used free-space protocol.

Much less research has been conducted for free-space QKD for short range links (less than 1m) and indoor spaces. One example of a practical, short range free-space QKD link is the financial transaction between a user with a handheld device and an Automated Teller Machine (ATM). The user uses a handheld device to exchange quantum keys with an ATM without the need to insert their bank card into the ATM. This prevents eavesdroppers from skimming bank card details and exposed pin codes. Experiments for this were reported in [55, 56, 132-134, 142-144].

An indoor free-space link that connected two optical fibres was reported in [103, 135]. This experiment showed the potential for ultra-high data rates (1.6 terabit/s) coexisting with the COW-QKD protocol, demonstrating secure wireless connectivity within an indoor space. The link operated over 2.5 m in free-space, in the presence of 200 lx background artificial illumination.

To the best of our knowledge there has been no work on short-range links suitable for operation both indoors (where the effect of sunlight is limited) and outdoors, and this is the focus of the work within this thesis, as detailed below.

1.5 Motivation and Aims for the Thesis

In this DPhil thesis we focus on secure communications techniques that ensure the quantum key is not intercepted and without using quantum entanglement. The work reported focuses on developing short-range links that are robust to sunlight. The BB84 protocol is chosen because the BB84 protocol was proven unconditionally secure and is well-suited to short-range links due to its straightforward implementation.

The key challenges that the work reported here addresses are

1. Mitigating ambient light noise, including selection of wavelength and verification of performance.
2. Developing tracking that can allow the link to operate given its narrow field of view.
3. Implementing the necessary transmitter and receiver subsystems.
4. Demonstrating link operation.

In the next chapter the operation and simulation of an indoor link is described in greater detail, with a focus on the effect of ambient light noise and its mitigation.

1.6 Summary

In this chapter, the need for privacy and security of data communication and information is established. Quantum Key Distribution (QKD) is a method to secure communications using Quantum Mechanics and the physical properties of light. A literature review of the relevant QKD protocols such as prepare-and-send, entanglement, and phase-based protocols was conducted. A literature review of long range and short range free-space QKD experiments that implemented prepare-and-send protocols and entanglement protocols was also conducted. These free-space links included outdoor experiments performed during nighttime and daylight, short range and indoor experiments, and operated in the visible light and near infrared wavelengths. The literature reviews showed that one of the key challenges with free-space QKD links is mitigating interference and induced noise from sources such as sunlight at the QKD detector. Sunlight is the main cause for noise in free-space QKD systems; hence, most long range free-space QKD links were performed at night. The long range free-space QKD links that performed in daylight required narrow passband spectral filters, extremely narrow fields of view, and spatial filtering using pinholes to reduce the sunlight at the QKD detector. The wavelengths of operation were typically in atmospheric transmission windows of 780 – 850 nm and 1550 nm that minimise the transmission loss and the interference from sunlight. The work reported in this DPhil thesis focuses on developing short-range QKD links that are robust to sunlight and implementing the BB84 protocol.

Chapter 2 Free-space QKD for Indoor Wireless Systems using BB84

In this chapter, a BB84 system model for indoor QKD communications in the presence of sunlight is developed. Noise models for artificial lighting and sunlight are detailed. QKD link simulations using QBER are then evaluated for two wavelengths in the visible light region.

2.1 BB84 Protocol

In the previous chapter, the BB84 protocol was described, and chosen as the most suitable protocol for an indoor free-space QKD link. The next sections describe important aspects of the BB84 protocol that are used for the indoor free-space QKD link model, simulations, and experiments reported in this thesis. These include the quantum bit error rate, attack methods by Eve, and mitigation techniques against those attacks.

2.1.1 Quantum Bit Error Rate

The standard QKD metric to detect an eavesdropper is the quantum bit error rate (QBER). In the BB84 protocol, after basis reconciliation Alice and Bob have a shared sifted key and the QBER is computed from the entire key. QBER is calculated as a ratio of the total number of errors to the total number of received photons and displayed as a percentage [29]. A common threshold for the BB84 protocol to operate correctly is 11% [30-32].

The Eq. (2) – (6) are used to estimate the QBER [29].

$$R_{sift} = \frac{1}{2}\, b\, f_{rep}\, \mu\, t_{link}\, \eta \tag{2}$$

$$R_{opt} = R_{sift}\, p_{opt} \tag{3}$$

$$p_{noise} = R_{noise}\,\tau, \qquad \tau \leq \frac{1}{f_{rep}} \tag{4}$$

$$R_{det} = \frac{1}{2}\frac{1}{2} f_{rep}\, p_{noise}\, n \tag{5}$$

$$QBER = \frac{R_{opt} + R_{det}}{R_{sift}} = p_{opt} + \frac{p_{noise} \cdot n}{t_{link} \cdot \eta \cdot 2 \cdot b \cdot \mu} \tag{6}$$

R_{sift} is the sifted raw key rate, R_{opt} is the intrinsic error rate of the QKD setup due to the probability of the sifted photon entering the wrong detector, R_{noise} is the total noise count rate (CPS) per detector, and R_{det} is the total noise count rate across all of the detectors. The parameters are coefficient $b = 1$ for non-phase coding setup, repetition rate f_{rep}, mean photon number μ, link transmission t_{link}, detector efficiency η, polarisation error p_{opt}, number of detectors n, gating window τ, and the probability of the total noise counts per detector within a gating window p_{noise}. The link transmission is the probability that a photon sent by Alice arrives at Bob's detectors. The total noise count rate per detector R_{noise} include dark counts and ambient light.

Dark counts and afterpulses contribute to the errors that make up the QBER and such errors can never be perfectly suppressed in practice. Therefore, the QBER should be minimised such that Alice and Bob can perform less error correction and privacy amplification to ensure the desired level of security.

2.1.2 BB84 Attack Methods

Eve can perform different types of attacks to gain information about the key. These attacks are the individual, collective, and coherent (generalised) attacks, photon number splitting attack, realistic beam splitter attack, and side channel attack.

2.1.2.1 Individual, Collective, and Coherent (Generalised) Attacks

Figure 3 is a diagram that shows the mutual information $I(A,B)$ and $I(A,E)$ vs the QBER [29]. This diagram only pertains to individual attack methods where Eve interacts with each qubit individually and independently (i.e. Eve captures qubits one at a time, measures her stored qubits individually and independently from each measurement). $I(A,B)$ is the mutual information between Alice and Bob and is calculated using the binary entropy function $H(z)$ with probability z [29].

$$H(z) = -z\log_2(z) - (1-z)\log_2(1-z) \tag{7}$$

$$I(A,B) = 1 - H(QBER) \tag{8}$$

For small QBER, the mutual information between Alice and Eve, $I(A,E)$, can be calculated using the approximation [29]

$$I(A,E) \approx 2.9QBER \tag{9}$$

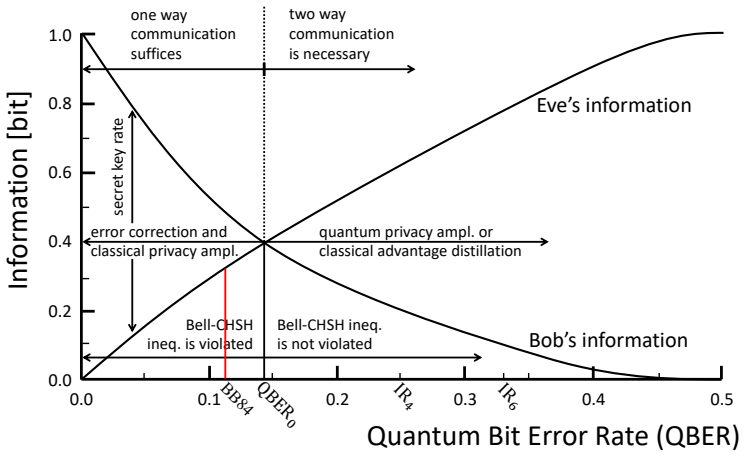


Figure 3: Diagram of mutual information between Alice and Bob $I(A,B)$ and Alice and Eve $I(A,E)$ vs QBER [29]. This diagram shows which methods to implement depending on how much information Eve knows compared to Bob. In the plot, the intersection of $I(A,B)$ and $I(A,E)$ occurs at $QBER_0 \approx 14\%$. At this intersection, Bob and Eve have the same amount of information about the secret key from Alice; hence, Eve probably knows the entire key.

There are two other types of attack methods Eve can perform: collective and coherent (generalised attack). A collective attack is when Eve can interact with each qubit independently and can measure the stored qubits as a group (i.e. Eve performs a joint measurement for all of the qubits simultaneously). This type of attack enables Eve to gain more information about the key compared to individual attacks. Security proofs against collective attacks are evaluated at the asymptotic limit (i.e. Alice and Bob have infinitely many rounds of a QKD protocol and Eve's collective attack is independent and identical for each round). These proofs are useful to understand how Eve might behave in a coherent or generalised attack. A coherent (generalised) attack is the most powerful type of attack Eve can perform. Eve can take control of the quantum channel, interact with every qubit before measuring them, store the qubits in quantum memory, and perform a collective attack on the group of qubits. The BB84 protocol was proven secure against individual attacks and the results are shown in [179-182]. The BB84 protocol was proven unconditionally secure against coherent (generalised) attacks with a maximum QBER threshold of 11% and the results are shown in [29, 36]. A practical QBER threshold to satisfy is 4% for a mean photon number $\mu = 0.1$. This threshold ensures that Alice and Bob have enough QBER margin to perform classical error correction and privacy amplification to guarantee security against Eve's individual attacks.

The goal is to have a finite size key that is secure against any attack. Proofs for the security against coherent attacks can be simplified to security against collective attacks with finite size keys [183]. This is a practical scenario for Alice and Bob where the shared sifted key length is not infinite (asymptotic limit) rather the key length is finite. The sifted key length must be long enough to allow for error correction, phase error estimation, and privacy amplification because in the process qubits are revealed for comparison over the public channel and must be discarded. The finite size security proofs in [184-189] proved the BB84 protocol has unconditional security against coherent attacks. The optimum coherent attack is a collective attack against the

BB84 protocol. This is not the same for other QKD protocols. The security proofs against coherent attacks for BB84 recommended finite size keys with a minimum key length of 10^5 qubits [184, 190, 191] and a maximum key length of 10^{12} qubits [188], which approaches the asymptotic limit. In this thesis, the sole focus of BB84 security is on individual attacks as they are simplest to analyse, proven secure with QBER = 11% limit, and security against individual attacks must be proven before proceeding to collective and coherent attacks.

2.1.2.2 Photon Number Splitting Attack

The Photon Number Splitting (PNS) attack is a type of intercept and resend strategy. Eve captures and stores away one of the multiple photons emitted from the WCP source. Eve lets the rest of the photons go to Bob. The PNS attack assumes Eve has a storage device with quantum memory to hold the excess photons. All of the photons emitted per pulse from the source have the same qubit information. As a result, Eve can learn about the key without having to interrupt the sequence of qubits. She can capture the photons while avoiding detection. Eve can store the photons away in her quantum memory to be deciphered later when Alice and Bob reconcile bases [29]. This is an individual attack because Eve will independently measure each photon as Alice and Bob confirm bases.

2.1.2.3 Realistic Beam Splitter Attack

A realistic beam splitter attack is when Eve intercepts all of the qubits between Alice and Bob. Alice sends pulses containing 0, 1 or 2+ photons per pulse (i.e. a multi-photon pulse) to Bob. Eve has enough photon counting devices that can measure all of these pulses in the H/V and D/A basis. The detectors must have nearly perfect quantum efficiency. Eve categorises the pulses into 0, 1, or multi-photon pulse. If a pulse has 2 or more photons, Eve keeps one and sends the extra photons to Bob. Otherwise, Eve does not send any photons to Bob. Essentially,

the realistic beam splitter attack is a more sophisticated intercept and resend strategy and gives Eve twice the information gain compared to the intercept and resend strategy.

A realistic beam splitter attack is different from a PNS attack. A PNS attack is where Eve obtains all information about the key from multi-photon pulses only and introduces no error. In a realistic beam splitter attack, the multi-photon pulses are the only pulses Bob receives from Alice via Eve. Therefore, no key can be extracted.

The mean photon number μ is a key parameter for WCP sources to ensure a secure QKD link. Alice and Bob should agree on the intensity of the pulse that maximises the probability of the single photon state when there is negligible link loss. One method to counter Eve is for Alice to lower her mean photon number μ such that Eve can only attack a fraction of the pulses with this beam splitter attack. If Alice lowers the mean photon number μ of the pulses (i.e. $\mu \leq 0.1$) she reduces the probability of multi-photon pulses; hence, this reduction will ensure Eve sends fewer photons over to Bob. However, dark counts will have a higher impact on the sifted key rate and the QBER would increase. This is a trade-off with security at the expense of key rate.

Paradoxically, the lower mean photon numbers can tolerate higher link losses (i.e. low transmissivity over the quantum channel). In practice, the maximum link loss that can be tolerated is a trade-off between the dark count rate and how low the mean photon number μ can be made (i.e. how many multi-photon pulses can be suppressed). The recommended mean photon number values for link losses 10, 14, and 20 dB correspond to $\mu = 0.25$, 0.1, 0.025, respectively [29]. In this thesis, a maximum threshold for link loss is set to 14 dB which corresponds to $\mu = 0.1$ for a realistic beam splitter attack.

2.1.2.4 Side Channel Attack

Side channel attacks gain information about the transmit sources from outside the quantum channel and directly from the transmitter implementation. In a BB84 optical setup, four WCP sources are used for the H, V, D, A polarisations and their temporal, spectral, and spatial domain properties should be indistinguishable. This prevents Eve from discovering which qubit came from which source. It is assumed Eve can gain mutual information with Alice from side channel attacks; hence in practice Alice's transmitter should minimise the differences in the temporal, spectral, and spatial domain properties of the WCP sources. In this thesis, a free-space BB84 QKD link experiment is implemented. Free-space QKD links are vulnerable to imperfect polarisation encoding and non-single-mode quantum signals. These issues are addressed and potentially mitigated in the final BB84 experiment.

There are mitigation techniques to protect against different types of attacks. Examples of such techniques for practical QKD implementations were reported in [192, 193]. One type of mitigation is to use a decoy state protocol with the BB84 protocol.

2.1.3 Decoy State Protocol

The decoy state protocol [194-201] was invented by Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen in 2005. This protocol enhances the detection of an eavesdropper by mitigating the PNS attack and increases the secure key rate for practical QKD links using weak coherent pulses (WCP). In the decoy state protocol, the WCP sources are modulated to send qubit pulses with varying intensities. There are three possible states: qubit signal pulse, dim pulse that is weaker than the signal (decoy state), and 'vacua' or near vacuum pulse that is weaker than the dim pulse (decoy state). The sum of the intensities for the decoy states is less than the intensity of the qubit signal pulse. The decoy state protocol can be used with two-states (signal state with a weaker or vacua state) or three-states (signal state with a weaker state and a vacua state). These

configurations are called one-decoy state and two-decoy state respectively. This protocol was proven to approach the asymptotic limit for key generation rates with three-states [202]. The BB84 and efficient BB84 protocols are typically used with two-decoy states because it is relatively simple to implement within the existing QKD system while also improving the key generation rates. Hence, the two-decoy state protocol is preferred in fibre [203-205] and free-space (e.g. satellite links [107, 108, 147]) experiments.

The decoy states are used for link security. For every qubit, Alice makes a random choice to send one of the three states to Bob over the quantum channel. Eve cannot distinguish between a signal state and a decoy state. After Bob measures all of the qubits, Alice tells Bob which states were the decoy states over the public channel and they separate their measurements based on signal and decoy states. Alice and Bob can determine whether eavesdropping occurred by using detection statistics of the different intensities to determine the weaker, vacua, and single photon component yields, and hence, the secure fraction of the detection events.

Non-decoy state protocols using WCP sources can only be used when there is low link loss [206]. In the current technology, non-decoy state protocols using WCP sources are susceptible to an intercept and resend strategy and the PNS attack. WCP sources must use weaker intensities for the qubit signal pulses (i.e. lower mean photon number) to reduce the probability of multi-photon pulses. This improves security against Eve's attack methods to gain information from multi-photon pulses (see section 2.1.2 for attack methods). However, the use of lower mean photon numbers reduces the key generation rate significantly and then the dominant factor in the QBER comes from the dark count rates of the detectors. There is a maximum limit for secure key rates (bits per channel use) on fibre and free-space QKD links in a lossy channel. In repeaterless quantum communications, the fundamental rate-loss scaling in a lossy channel is set by the PLOB bound named after Stefano Pirandola, Riccardo Laurenza,

Carlo Ottaviani, and Leonardo Banchi [207]. This bound sets the maximum achievable rate limit for secure key rates without quantum repeaters and is calculated by

$$C(\eta) = -log_2(1-\eta) \quad , \quad 0 \leq \eta \leq 1 \tag{10}$$

$$C(\eta) \cong 1.44\eta \quad , \quad \eta \cong 0 \tag{11}$$

where $C(\eta)$ is the secret key capacity (bits per channel use) and η is channel transmissivity. Eq. (11) is approximately 1.44η bits per use in a high loss quantum channel when η is approximately zero. The ideal BB84 protocol using single photons has a maximum secret key capacity of $\frac{\eta}{2}$ bits per channel use. The BB84 protocol with WCP sources and decoy states has a maximum secret key capacity of $\frac{\eta}{2e}$ bits per channel use.

In this thesis, the indoor QKD link model, simulations, and experiment are for a BB84 system without any decoy state protocol.

2.2 Choice of Wavelength

The choice of wavelength is the key to all QKD systems. Ideally, a free-space QKD system would operate in a wavelength region with no interference or noise. In practice, most free-space QKD links operate in wavelength regions with photon counts from sunlight that are orders of magnitude greater than a single photon. Typically, free-space QKD systems are not pointed directly at the Sun because the wavelengths of operation used are not naturally resilient to sunlight and a high number of photon counts from sunlight interfere and induce noise at the QKD detector. Most outdoor free-space QKD links operate within atmospheric transmission windows (e.g. 780 – 850 nm and 1550 nm) that minimise the transmission loss and the interference from sunlight at the QKD detector. Short range free-space handheld QKD links have also operated at wavelengths around 850 nm [56, 142-144].

It is challenging to operate a free-space QKD link in the presence of sunlight at visible wavelengths. Examples of visible light free-space QKD experiments that have operated between 600 – 700 nm are short range free-space handheld QKD links operated in a laboratory (632 nm [132], 650 nm [133, 134], and 658 nm [55]), an outdoor free-space QKD link operated at night [121], and an indoor free-space QKD link operated in a laboratory with daylight through a window [116]. The experiment in [121] was a free-space BB84 QKD link demonstrated at night between two buildings 1.38 km apart. The transmitter operated at 650 nm for the quantum channel. The main analysis of this work was to analyse the effect of atmospheric turbulence on the clock signal and how much time drift affected the QBER of the link. The free-space BB84 QKD link experiment in [116] was operated in a laboratory with a window that allowed sunlight to enter. The transmitter and receiver were positioned in front of the window such that the receiver was pointed at the window (daylight with cloudy skies). The operating wavelength of the transmitter was 670 nm. The receiver consisted of a 10 nm bandwidth interference filter and a spatial filter that narrowed the FOV to reduce the background daylight counts on the detectors. The spatial filtering was the biggest factor to reduce the background counts to enable the QKD link to work.

However, there is an atmospheric absorption region that has minimal photon counts such as the water and carbon dioxide absorption band between 1351 – 1414 nm [208]. This is a potential novel wavelength region to investigate for an indoor free-space QKD link because of the extremely low photon counts from sunlight and the relative flatness of the region. These two factors could relax the constraints on the types of spectral filters used and the spatial filtering techniques currently used for free-space QKD links. The relative flatness of the region between 1351 – 1414 nm could enable the use of a larger passband filter to increase the FOV of the QKD receiver. The increased FOV of the receiver can reduce pointing and alignment issues and improve the mobility of the QKD receiver. The photon counts from sunlight are minimal

between 1351 – 1414 nm. Theoretically, the QKD receiver can be in direct sunlight with minimal interference. This could relax the constraints on spatial filtering and reduce the complexity of the QKD receiver configuration.

Also, there is a potential benefit to integrate wavelengths of operation between 1351 – 1414 nm to improve the compatibility with telecommunications wavelengths in existing fibre networks. Fibre communications were limited in the full utilisation of the spectrum from 1310 – 1550 nm due to impurities in silica fibres. However, recent advances in fibre technologies have removed the hydroxyl (OH-) ion absorption or 'water peak' at ~1383 nm in single mode fibres [209, 210]. The full spectrum from 1310 – 1550 nm can now be fully utilised with minimal losses in commercial fibres. Wavelengths from 1351 – 1414 nm are in close proximity to telecommunications wavelengths. These wavelengths in the E-band can be used in fibre networks using CWDM (Coarse Wavelength Division Multiplexing). Each wavelength can be recovered through filtering [211-215]. Moreover, fibre-only architectures can evolve to fibre-wireless-fibre architectures such that central network offices connect to their satellite offices via fibre and use indoor optical wireless communications for their end-users [103, 135].

There are potential engineering trade-offs when designing an indoor free-space QKD link. Such a link is wavelength dependent, and the engineering design decisions are based on the availability of the components, size, cost of equipment, and the potential integration with telecommunications networks and other systems at the wavelength of operation. Transmitter and receiver components are typically available in the visible and near infrared wavelengths. The wavelength compatibility with visible light communication (VLC) systems [216, 217] and telecommunications systems may be challenging. VLC systems utilise wavelengths between 380 – 750 nm and there is potential interference from other VLC sources and LED lighting

used for illumination. Telecommunications wavelengths are typically 850 nm, 1310 nm, and 1550 nm and these wavelengths can be limiting factors in the engineering design.

The design of the QKD transmitter should consider sources, optics, and electrical equipment (driver circuits, temperature controllers, power supplies, etc.). Sources such as LEDs and lasers come in a wide range of wavelengths and power levels, can be cost effective, capable of high data rates, and come in a range of sizes depending on the manufacturer. Optical components are available in a wide range of coatings from narrowband to wideband spectra, come in select sizes depending on the manufacturer, and can be expensive. Electronic equipment come in a range of sizes and can be expensive depending on the manufacturer. The design of the QKD receiver should consider detectors, optics, and electrical equipment. Detectors are designed for a specific range of wavelengths, thermal noise level, and photon detection efficiency (PDE). The detectors with low thermal noise and high PDE can be expensive. The detectors come in a range of sizes depending on the manufacturer and technology used. The design considerations for the optics and electrical equipment for the receiver are similar to that of the transmitter.

2.3 Indoor System Model for QKD

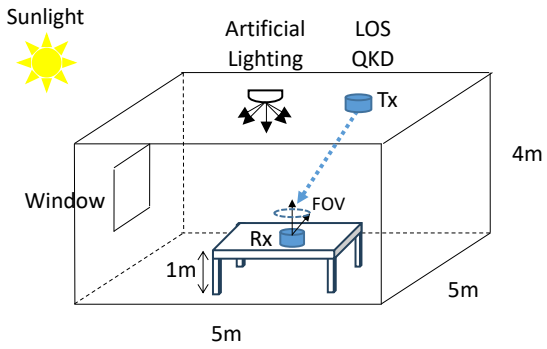


Figure 4: System overview of an indoor free-space QKD link in the presence of artificial lighting and sunlight.The free-space QKD link is line of sight (LOS) between a transmitter (Tx) on the ceiling and a receiver (Rx) on a desk. The receiver has a field of view (FOV). Within this FOV, the Rx is exposed to the QKD signal and illumination from ambient light sources such as artificial lighting and sunlight through a window.

A model is developed to simulate the effect of ambient light on a QKD receiver and its effects on an indoor free-space QKD link are assessed. Figure 4 shows an indoor free-space QKD link within a typical room. The room has dimensions 5 x 5 x 4 m (L x W x H) with artificial lighting on the ceiling and a window which allows sunlight to illuminate the room. The free-space QKD link is a Line Of Sight (LOS) link consisting of a transmitter (Tx) on the ceiling and a receiver (Rx) on a desk. The transmitter sends signals at single-photon level to the receiver. Weak coherent pulse (WCP) sources are considered at the transmitter. The receiver measures the photons within a detection window (gating window) using a photon counting device. In the room, ambient light consists of artificial lighting and sunlight. This represents the major potential link impairment and the model is developed to understand the effect this has.

Figure 5 shows a typical implementation of an indoor free-space QKD link. The transmitter consists of WCP sources, a BB84 transmitter, a lens with a focal length equal to the distance between the transmitter and receiver, and an aperture to control the Airy Disk which is incident

at the receiver. The receiver consists of an entrance pupil, a spectral filter, a BB84 receiver, and QKD detectors. The receiver is etendue-limited with a field of view (FOV) with half angle Ψ_c. It is assumed that the received photons arrive incident at the receiver within the receiver's FOV. Two types of detectors are used in the model: 1) a multimode fibre-coupled single photon detector with a collimator at the front end and 2) a single mode fibre-coupled single photon detector.

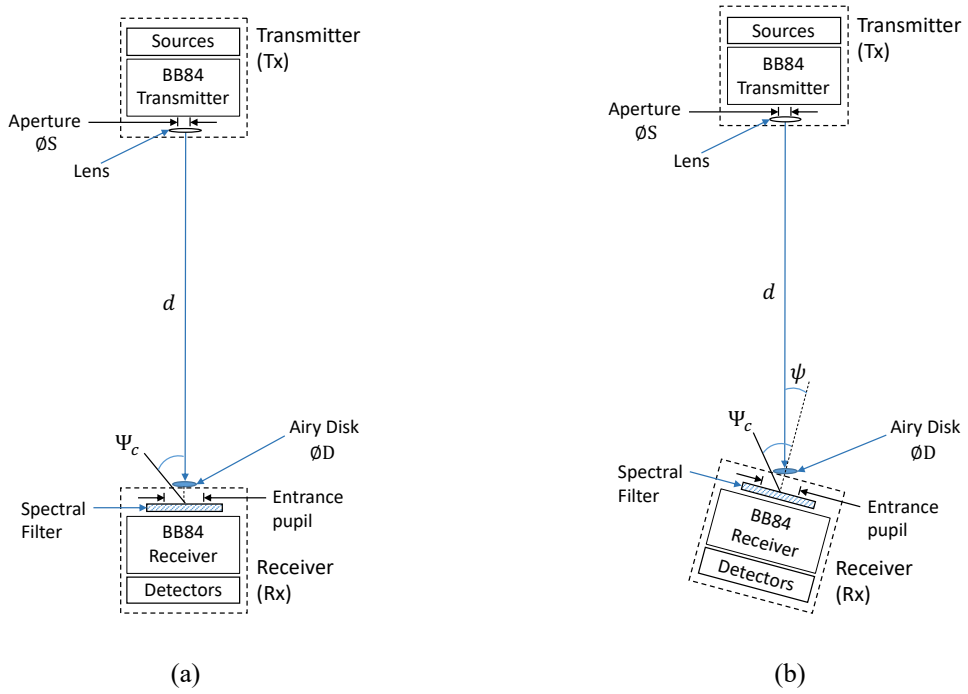


Figure 5: Diagram of an indoor free-space BB84 link. (a) The transmitter (Tx) is located at a distance d above the receiver (Rx). At the Tx, the lens has a focal length equal to the distance d to the Rx. This allows the Tx to transmit a first order Airy disk beam spot which is incident on the Rx. The aperture, with diameter ØS, can be adjusted to change the beam diameter ØD of the Airy disk. The Rx has a field of view (FOV) with half angle Ψ_c. (b) This diagram shows the receiver setup rotated with an angle of incidence (AOI) ψ.

In the QKD link model, it is assumed the transmitter and receiver can track each other to ensure that a link is maintained. This involves pointing the transmitter at the receiver and vice-versa, in order to ensure light is incident on the receiver within its field of view (see [176-178] for

possible implementations of tracking systems). (In the final experimental setup, the transmitter and receiver are manually aligned and pointed at each other to ensure a line of sight link.) In the following sections, we describe each of the components of the model in detail and specify hardware options at the transmitter and receiver.

2.3.1 Transmitter

2.3.1.1 Source Options

The transmitter would ideally be a single photon source [105, 106, 140, 141, 218] that generates a single photon on demand with a probability of 1. However, a weak coherent pulse (WCP) source is more realistic and more common in experimental implementations of QKD systems. A WCP source, for example an attenuated laser or LED, may generate two or more photons per pulse in accordance with the Poisson distribution. Such a weak coherent source follows a Poisson Cumulative Distribution Function where probability that up to x photons arrive within a time interval is [219]

$$P(X \leq x) = \sum_{k=0}^{x} \frac{\mu^k e^{-\mu}}{k!} \tag{12}$$

In Eq. (12) μ is mean photon number and k is the number of photons within the interval. Figure 6 shows the probability of photon generation vs number of photons per pulse for a WCP source. Typically μ is set to 0.1. It can be seen in Figure 6 that higher values of μ generates more multi-photon pulses.

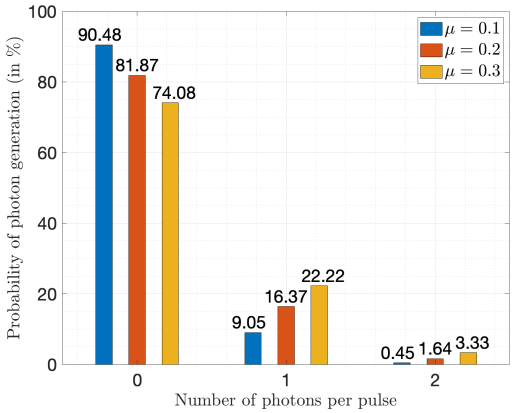


Figure 6: Plot of the probability of photon generation vs number of photons per pulse for a WCP source. The increase in mean photon number μ increases the probability of multi-photon pulses.

LEDs and lasers have both been used as WCP sources for QKD. Examples of free-space QKD links using LEDs [55] and lasers [149] have been reported. LEDs can be driven using current or voltage drivers and are difficult to operate at high pulse rates given their limited bandwidth. LEDs, however, have broad spectra and do not require temperature stabilisation to achieve a particular wavelength. A spectral filter with a narrower bandwidth than the emission spectra of the LED source can be used at the output of a QKD transmitter to ensure the LED sources have the same spectral profile. This ensures the LED sources are spectrally indistinguishable which is necessary to mitigate side channel attacks. Contrary to LEDs, lasers can operate at high pulse rates. However, lasers have narrowband spectra and require more complex drivers and temperature stabilisation to ensure the same spectral profile of the laser sources.

2.3.1.2 BB84 Transmitter Model

The QKD link is modelled with a transmitter sending signals at single-photon level to a receiver. Figure 7 shows a general design of a BB84 transmitter.

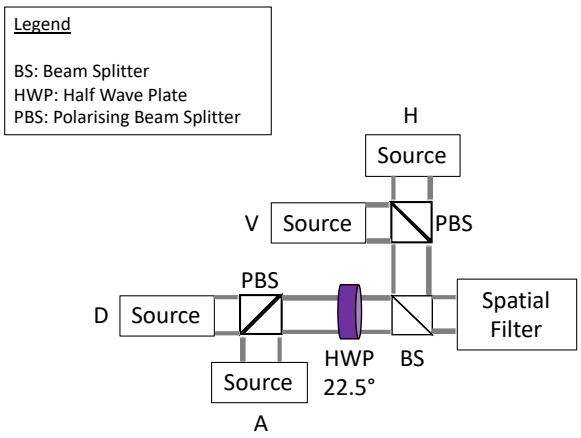


Figure 7: General BB84 transmitter design[114]. In the optical setup, the output of each source is collimated. Each polarisation basis consists of a high extinction polarising beam splitter (PBS) where the transmitted beam is horizontal linearly polarised light and the reflected beam is vertical linearly polarised light. At the output of the D/A polarisation branch is a half wave plate (HWP) set to 22.5˚ which rotates these polarisations to 45˚ (A) and 135˚ (D). The H/V and D/A branches combine at the 50:50 non-polarising beam splitter (BS). The output of the non-polarising beam splitter is sent through a spatial filter to ensure all of the transmitted signals are spatially indistinguishable i.e. beam profile and beam shape.

The transmitter transmits a diffraction-limited beam that creates an Airy disk with beam diameter ($\emptyset$D) at the receiver plane [220]. In the model, the receiver is on a desk that has a height of 1 metre. The transmitter is above the receiver at $d = 3$ metres and the focal length of the lens at the output of the transmitter is equal to distance d. In the room, the furthest distance from the centre of the ceiling to a desk that is located at the corners of the room is approximately equal to 3 metres; hence the focal length of the lens is fixed at $d = 3$ metres. It is assumed that a flat-top intensity profile is at the output of the transmit aperture to create an Airy disk pattern at the focal length of the lens. The size of the Airy disk beam is given by

$$\emptyset\mathrm{D} = \frac{2.44\lambda_0 d}{\emptyset\mathrm{S}} \tag{13}$$

where λ_0 is transmit wavelength, d is the distance between the transmitter and receiver, ∅D and ∅S are the circular diameters of the Airy disk beam and source's aperture respectively. The source apertures are adjusted to create Airy disks of ∅1, 2, and 3 mm at the receiver plane.

2.3.2 Receiver

2.3.2.1 Detector Options

The basic detection scheme of any QKD receiver is to use a single photon detector to count photons. There are several types of photon detectors: superconducting nanowire single photon detectors (SNSPDs), linear avalanche photo diodes (APDs), and single photon avalanche diodes (SPADs). Superconducting nanowire single photon detectors (SNSPDs) [221, 222] are made up of wires that are 10's of nanometres wide (i.e. one detector is approximately 100 nm wide by 100 μm long) with a readout amplifier. The detector must be cooled to cryogenic temperatures (i.e. below the superconducting critical temperature of the nanowires) and the current is DC biased to just below the superconducting critical current. When a photon is detected, a resistance is created inside the nanowires. The DC bias current flows across this resistance to the readout amplifier and is registered as a voltage (photon count) at the detector. After the current flows away from the nanowires, the temperature drops back to below superconducting levels and the detector is ready to detect again. SNSPDs have three advantages: very high quantum efficiency, low dark count rate, and low timing jitter. However, they are very expensive and require cryogenic temperatures which limits their applications in practical settings.

Linear APDs [223-225] are avalanche photo diodes that are reverse biased below the breakdown voltage and utilise the exponential charge multiplication of an avalanche. This is a surge in current from the accelerated movement of charge carriers in the p-n junction due to the electric field. This operating region is linear where the received signal is proportional to the

input signal. As a result, the received signal is very low when measuring single photons. Consequently, linear APDs are used with a transimpedance amplifier that converts the photocurrent into a voltage and amplifies the signal. Linear APDs are typically used in high bit-rate (GHz) fibre QKD systems [226-231].

A Single Photon Avalanche Diode (SPAD) [219, 232-234] is a photo diode that operates in Geiger mode where the p-n junction is reverse biased well above the breakdown voltage. The operation of the SPAD also utilises the exponential charge multiplication of an avalanche. However, in Geiger mode, the electric field across the p-n junction is so high that the avalanche is self-sustaining. An avalanche current can be generated from a single photon absorbed in the active area and creating an electron-hole pair. The electron and hole (charge carriers) are accelerated towards the p and n sides respectively due to the high electric field within the junction. The acceleration of the charge carriers can free more carriers through impact ionisation. The result is an avalanche current which the device registers as a photon count. Afterwards, the SPAD is reset with a quenching circuit that dissipates the current and brings the bias voltage below the breakdown voltage. The SPAD cannot count any more photons until the SPAD is recharged with a bias voltage that is well above the breakdown voltage. This process of recharging the SPAD is known as the dead time.

In a SPAD there are two types of thermal-generated noise: dark counts and afterpulses. A dark count is caused by a spontaneous avalanche current that occurs in the p-n junction when the SPAD is in the dark and without illumination. Dark counts follow a Poisson distribution and increase with temperature. The probability of a dark count also increases with increased excess bias voltage above the breakdown voltage. Two methods to reduce the dark counts are to cool the SPAD and to operate at a lower excess bias voltage at the expense of decreased photon detection efficiency (PDE). Afterpulses are caused by the release of temporarily trapped charge

carriers in the p-n junction. If the SPAD is not fully quenched, the trapped carriers may be released during the next active detection period of the SPAD. After the SPAD has recharged with a bias above the breakdown voltage, the high electric field may release the trapped carriers to create an avalanche current that would register as a photon count. Two methods to reduce afterpulses are to increase the dead time between detection events to allow the SPAD to be fully quenched and to operate at lower electric fields [232].

SPAD modules are used in a variety of QKD applications in fibre [32, 82, 124, 126, 200, 203-205, 211, 229, 235-239] and free-space links [51, 53, 55, 56, 81-84, 87-90, 105, 107-114, 116-120, 128-133, 135, 137-141, 143-145, 147, 150-153, 161, 162, 165-167, 240-242]. SPAD modules can be made compact and are suitable for indoor spaces such as office and room environments. A SPAD module can operate in two modes: gated mode and free-running mode. In gated mode, a SPAD module uses a 'gating window' which is a short time period (e.g. 1 ns) when the diode is active to detect photons. The diode is inactive and does not register a photon count outside of the gating window. The advantage of this mode is its effectiveness to reduce the noise at the detector. Gated mode is typically used when the link between the transmitter and receiver is synchronised for single photon detection. In free-running mode, a SPAD module does not use a gating window. Instead, the gate signal for the SPAD module is always set to the 'active state' and the diode is always on. In this mode, the detector noise is higher compared to gated mode, however free-running SPAD modules can be used in an asynchronous link.

The photon detection efficiencies (PDE) of SPAD modules vary depending on the detector types. SPAD modules with silicon detectors that operate in the visible region can have a PDE up to 85%. SPAD modules with InGaAs detectors that operate in the near infrared region (NIR) between 900 – 1700 nm can have a PDE of up to 25%. Figure 8 shows the detector characteristics of a typical NIR SPAD module (idQube [243]). Figure 8a shows the PDE as a

function of wavelength for a idQube detector. Figure 8b shows the dark count rate and the detector jitter as a function of PDE.

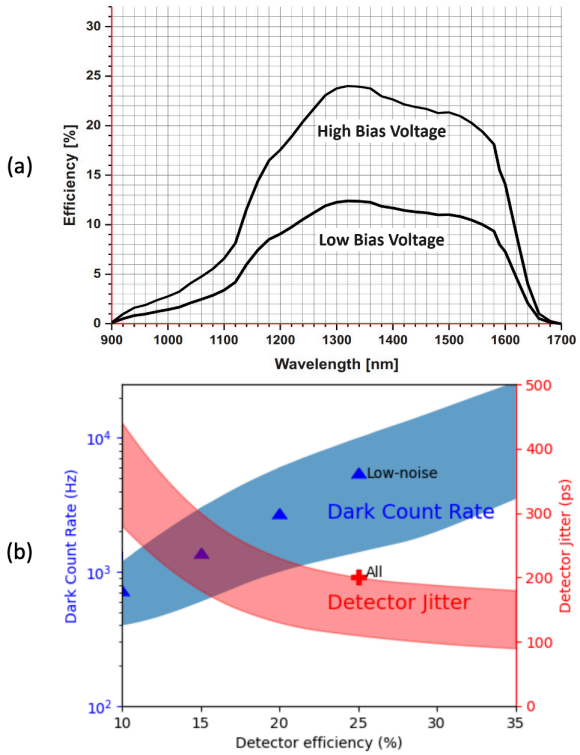


Figure 8: Plots of the detector characteristics for a typical NIR SPAD module. The graphs in this figure were taken from the ID Quantique idQube datasheet [243]. (a) PDE vs wavelength. The two curves represent the PDE of the SPAD when using high and low bias voltages. The SPADs are typically set to a higher voltage to obtain the higher PDE. (b) Dark count rate vs PDE (left axis) and Detector jitter vs PDE (right axis). SPADs that operate with higher PDE typically have higher dark count rates and higher probability of afterpulses. (The low-noise idQube model was used for NIR measurements and experiments reported in this thesis).

2.3.2.2 BB84 Receiver Model

In a BB84 link a QKD receiver can have a similar structure to a QKD transmitter. The receiver (Rx) can consist of a spectral filter, optical components such as beam splitters and waveplates, and single photon detectors. Figure 9 shows a general design of a BB84 receiver.

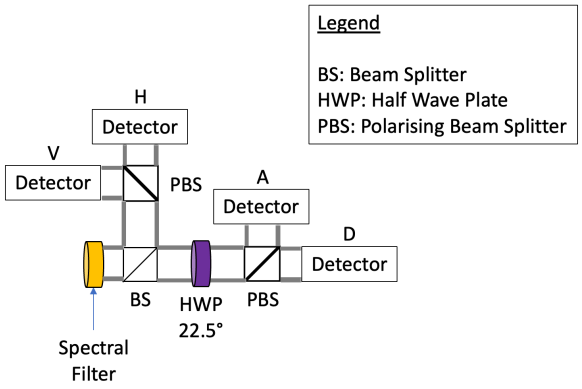


Figure 9: General BB84 receiver design[114]. The receiver design is based on the BB84 protocol. At the entrance of the receiver, a spectral filter is used to mitigate the ambient light entering the receiver. The basis selection is performed in the optical setup. A non-polarising 50:50 beam splitter is used to facilitate Bob's choice of basis pair. One path of the receiver consists of a polarising beam splitter to choose between Horizontal and Vertical outcome. The other path consists of a half wave plate and polarising beam splitter to choose between Diagonal and Anti-diagonal outcome. The number of photons detected at each detector is estimated based on the receiver design. Each detector receives an equal number of photons (for the standard BB84 protocol, but not the efficient BB84 protocol with biased basis choice).

The receiver has an etendue that is limited by the collection area and field of view of the detector. Etendue [244] should be conserved such that

$$\mathrm{A}_{eff}\Omega_{eff} \leq \mathrm{A}_{det}\Omega_{det} \tag{14}$$

$$\frac{\pi}{4}(\emptyset\mathrm{F})^2 2\pi(1-\cos\alpha) \leq \frac{\pi}{4}(\emptyset\mathrm{G})^2 2\pi(1-\cos\Psi_c) \quad , \quad 0 < \alpha \leq \Psi_c \tag{15}$$

where A_{eff} is the effective area of the entrance pupil, Ω_{eff} is the solid angle of the entrance pupil, A_{det} is the detector collection area, Ω_{det} is the solid angle of the detector, $\emptyset\mathrm{F}$ is the diameter of the entrance pupil, α is the half angle FOV of the entrance pupil, $\emptyset\mathrm{G}$ is the diameter of the detector, and Ψ_c is the half angle FOV of the detector. The solid angles are the maximum FOV for the receiver and only light that enters within this solid angle can pass through to the detector.

2.3.2.3 Methods to Reduce Noise at the Receiver

A key challenge for an indoor free-space QKD link is to mitigate the effects of artificial lighting and sunlight at the receiver. There are three methods to reduce the noise and interference from ambient light on the receiver: use time gating techniques, minimise receiver etendue, and narrowband spectral filtering.

- The time gating technique is a 'gating window' or short time period when the detector is on and expects to receive a signal. Typically, the gating window is set to the transmitter signal period after Alice and Bob have synchronised over the public channel. Examples of experiments with free-space QKD receivers that operated within a gating window of 5 ns were reported in [111, 113].

- The receiver etendue should be minimised to limit the noise that enters the receiver. This usually consists of a narrow FOV and small detector collection area. As an example, a practical free-space QKD experiment that used a field of view of 0.1˚ and a detector collection area of 5 mm^2 was reported in [55].

- Spectral filtering defines the wavelength region of interest where the receiver rejects any signal outside of this region. The receiver should use a narrowband filter to reduce the spectral power of ambient light. Examples of experiments with free-space QKD receivers that used a narrowband filter of one nanometre were reported in [112, 115]. The wavelengths used in these references are 773 nm and 633 nm respectively. The next section details how spectral filtering is implemented in the model.

2.3.2.4 Spectral Filter

The receiver model uses a spectral filter to limit the amount of ambient light and allows a narrow range of wavelengths to be transmitted to the detector. The spectral filter bandwidth $\Delta(\psi)$ must be designed to ensure the transmit wavelength λ_0 remains within the passband for a range of angles from 0˚ to ψ. This leads to an increase in the optical bandwidth of the system as the FOV of the link increases. The filter has a spectral transmittance (F_T) at a central filter wavelength longer than the transmit wavelength λ_0. The filter passband shifts to shorter wavelengths when the angle of incidence ψ increases [245]. The wavelength shift is given by

$$\lambda(\psi) = \lambda_0 \sqrt{1 - \left(\frac{\sin\psi}{n_e}\right)^2} \quad , \quad 0 \leq \psi \leq \Psi_c \tag{16}$$

where λ_0 is the transmit wavelength, ψ is the angle of incidence, Ψ_c is the half angle FOV of the detector, and n_e is the effective refractive index of the spectral filter.

Figure 10 shows how increasing the bandwidth of the filter can increase the FOV of the filter. The figure also shows how the filter passband changes as the angle of incidence increases.

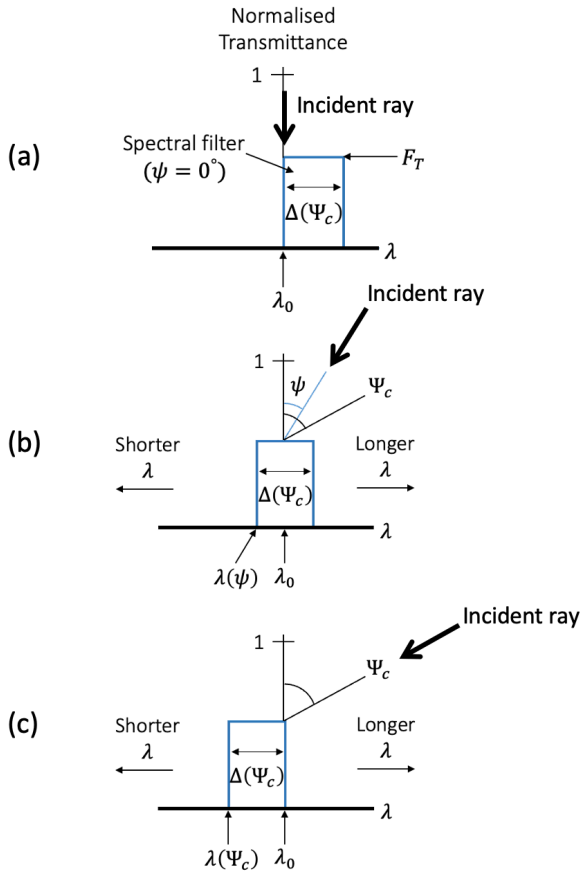


Figure 10: Diagram of spectral filter passband shift and FOV.(a) The filter passband should be designed with the transmit wavelength as the lower end of the passband to maximise the FOV of the filter. (b) The filter passband shifts to shorter wavelengths as the angle of incidence increases. (c) The longest wavelength allowed is the transmit wavelength and this occurs at the maximum half angle FOV Ψ_c. The spectral filter with a larger bandwidth has a larger FOV for the transmit wavelength to pass.

The QKD link simulations in section 2.5 and section 2.6 use visible wavelengths 658 nm and 761 nm respectively. Figure 11 shows the bandwidth of the spectral filter designed for increasing half angle FOV Ψ_c for these two wavelengths. Using Eq. (16), $\lambda_0 = 658$ nm or 761 nm in the visible region with n_e = 1.5 for a typical visible filter [246-248]. It can be seen in Figure 11 that increased angles requires a wider bandwidth to ensure the desired wavelength passes through the filter.

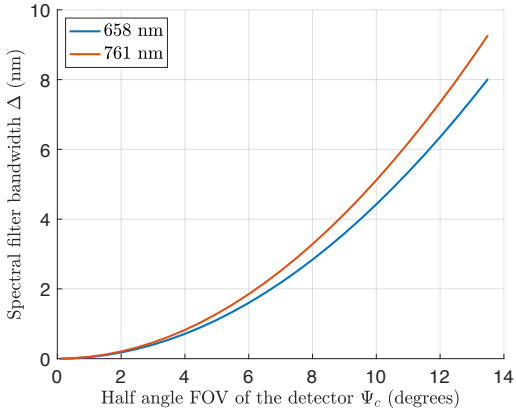


Figure 11: Plot of spectral filter bandwidth Δ vs half angle field of view of the detector Ψ_c for two wavelengths in the visible region of the optical spectrum.

2.3.3 Geometrical Link Loss

A simple link loss model is developed to determine whether a QKD link would work. The received signal link loss is approximated using the geometrical loss from the effective area of the entrance pupil and the Airy disk beam area. The beam spot is the Airy disk (central beam spot up to the first minimum of the Airy disk pattern) located at the entrance pupil of the receiver. It is assumed the power within the Airy disk beam is uniformly distributed across the beam. Link loss in dB (L_L) is estimated as the ratio of the effective area at the receiver over the Airy disk beam area. If the Airy disk beam area is within the effective area, then $L_L = 0$ dB and there is no link loss.

$$L_L = \begin{cases} 0 \quad , \quad if \quad \dfrac{\mathrm{A}_{eff}\cos\psi}{\frac{\pi}{4}(\emptyset\mathrm{D})^2} \geq 1 \\ 10log_{10}\left(\dfrac{\mathrm{A}_{eff}\cos\psi}{\frac{\pi}{4}(\emptyset\mathrm{D})^2}\right) \quad , \quad else \end{cases} \tag{17}$$

where A_{eff} is the effective area of the entrance pupil, $\emptyset\mathrm{D}$ is the Airy disk beam diameter, and ψ is the angle of incidence.

There are two limitations of this geometrical link loss model: 1) the intensity profile at the transmitter may not be a flat-top depending on the size of the aperture and the distance from the aperture to the source and 2) a non-negligible fraction of the beam beyond the first minimum of the Airy disk can contribute to the received signal. An improvement to the link loss model is to use a truncated Gaussian intensity profile at the output of the transmit aperture. A truncated Gaussian intensity profile in the far field is a convolution of Gaussian and Airy beam distributions. For the purpose of a simple approximation, the link loss model using the Airy disk beam spot is sufficient to determine whether a QKD link would work.

2.3.4 Link impairments

Artificial lighting can impair the performance of wireless QKD in indoor environments. Impairments due to LED lighting only were investigated [249, 250] previously. The work in [249] was a simulation of a windowless room with an LED light as the only source of noise and interference for the QKD system. The operating wavelength was 880 nm with the QKD transmitter on the floor and the QKD receiver at the same height as the LED lighting. The interference from the LED lighting was only considered from reflections off the walls and floor (potentially carpet) with no direct illumination on the receiver. This was not a practical scenario. The paper does not use polarisation-based BB84; rather it simulated several scenarios using a phase-based version of BB84 with biased bases, BB84 with decoy states, and RFI-QKD. The phase-based version of BB84 was similar to DPS-QKD where the QKD signals were time-bin encoded and the difference in the phases of consecutive pulses resulted in the basis. The QKD signals were filtered, decoded with a Mach-Zehnder interferometer, and time-binned in 100 ps at the two single photon detectors. The conclusions of the paper were that wireless indoor QKD was feasible in a windowless room lit by an LED source. There existed a regime or scenario where quantum keys could be generated in indoor environments. Minor alignment issues could be mitigated with beam steering techniques.

The simulation in [250] expanded on the wireless indoor QKD link model in [249] where a quantum user in a wireless indoor QKD environment had access to a fibre network to a central office. This hybrid quantum-classical network consisted of a wireless indoor QKD link and a fibre-based passive optical network (PON) that could use dense wavelength division multiplexing (DWDM) to carry quantum and classical data over the same fibres. The operating wavelengths were 880 nm for the quantum channel and a range of wavelengths around 1550 nm for the classical channel. The noise and interference model (LED lighting only) for the wireless indoor QKD link were the same as in [249]. The source of noise and interference in the fibre network was the Raman scattering. The Raman noise was generated by a strong signal from the classical data channel and spanned over a wide range of frequencies. This could potentially cause unwanted single photon detection at the QKD receivers. The protocols simulated were decoy state BB84 with biased bases, MDI-QKD, and CV-QKD. The conclusions of the paper were LED lighting and Raman noise were significantly higher than the dark counts of the single photon detectors and caused the most interference on the two types of links. Dynamic beam steering at the transmitter and receiver should be implemented to improve the link loss. Each protocol had its advantages and disadvantages depending on the scenario.

The deficiencies in the indoor QKD link models in [249, 250] were the windowless room with LED lighting only and an impractical indoor QKD link configuration where the receiver was on the ceiling. The receiver did not get direct illumination from the LED lighting, only reflections off the wall and floor. These deficiencies were overcome in the models used in this thesis. A practical scenario is a room with a window that allows sunlight to enter. There can be both LED lighting and sunlight for indoor environments. Illumination from the Sun can be much stronger than any artificial illumination and is potentially the main cause of impairment

of the QKD link. The transmitter is on the ceiling and the receiver is on a desk. This configuration exposes the receiver to all of the ambient light in the room. The following sections describe models for artificial lighting and sunlight.

2.3.4.1 Artificial Lighting Model

The artificial lighting model used in the simulations here assumes that an LED source uniform illuminates the room with average luminance of 500 lx, which is suitable for a reading environment. A typical LED light bulb has parameters shown in Table 1 and a plot of normalised relative intensity shown in Figure 12.

Table 1: Typical LED light bulb emission parameters.

Cree LED BR30 Flood Light (1 Bulb) [251]	
Colour temperature (Kelvin)	2700 (Soft-White)
Electrical power (Watts)	9.5
Brightness (Lumens)	650
Optical power (Watts)	0.95

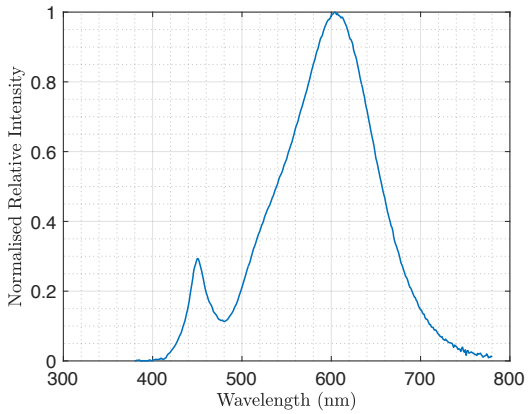


Figure 12: Plot of normalised relative intensity vs wavelength of one Cree LED bulb.The blue LED has an excitation wavelength at 450 nm and the yellow phosphor has an emission peak at 604 nm [251].

This light source is modelled as a point source located at the centre of the ceiling and $d = 3$ metres from the QKD receiver. In the link model, it is assumed the LED is co-located with the QKD transmitter. The LED is a Lambertian source with 60˚ half power semi angle (Lambertian order m = 1) to distribute the light to the edges of the room. In order to estimate the power, the LOS power at the receiver is calculated by [252]

$$P_{R,LED} = U(0)L_{LED} \tag{18}$$

$$U(0) = \begin{cases} (m+1)\,(cos\,\theta)^m\,\mathrm{A}_{eff}\Omega_{eff}\,cos\,\psi & , \quad 0 \le \psi \le \Psi_\mathrm{c} \\ 0 & , \quad \psi > \Psi_\mathrm{c} \end{cases} \tag{19}$$

$$L_{LED} = \frac{P_{T,LED}}{2\pi d^2} \tag{20}$$

where $P_{R,LED}$ is the power received, $U(0)$ is the transfer function, m is the Lambertian order, θ is the angle with respect to normal of the source, A_{eff} is the effective area of the entrance pupil, Ω_{eff} is the solid angle of the entrance pupil, Ψ_c is the half angle FOV of the detector, ψ is the angle of incidence, L_{LED} is the filtered LED radiance ($\mathrm{W.m^{-2}.sr^{-1}}$), $P_{T,LED}$ is the power transmitted, and d is the distance from source to receiver.

The output power of the LED is chosen to sufficiently illuminate a desk with an average intensity of 500 lx at a distance of 3 metres. This requires 7 bulbs, with approximately 7 W of optical power. This is estimated by integrating the product of the photopic luminosity function and the LED spectrum in Figure 12. The total luminous flux is divided by the distance squared and this results in the lux level emitted from one bulb onto the desk. This power estimation assumes that a flat detector with 2π steradian FOV was used. Figure 13 shows the spectrum of the LED model in $\mathrm{photons.s^{-1}.m^{-2}.sr^{-1}.nm^{-1}}$ vs wavelength. Figure 13 was created by scaling Figure 12 to the optical power of one CREE LED bulb (BR30) at 3 metres.

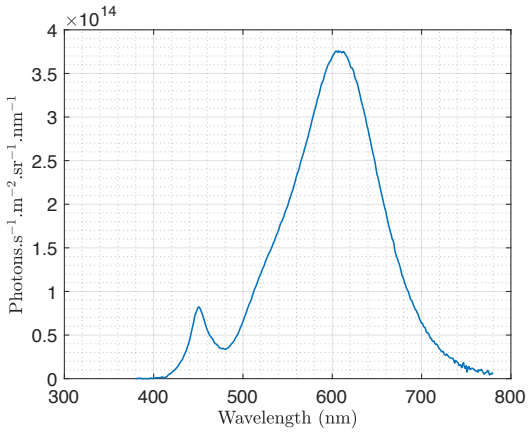


Figure 13: Plot of photons.s^{-1}.m^{-2}.sr^{-1}.nm^{-1} vs wavelength of the LED model.

2.3.4.2 Sunlight Model

The sunlight model uses the ASTM Air Mass 1.5 (AM1.5) standard for the spectral irradiance (W. m^{-2}) of sunlight at sea level with cloudless atmospheric conditions [253-256]. The ASTM AM1.5 standard is a spectrum of the average solar irradiances in 2π steradian FOV measured across several observatories in the continental United States. (AM1.5 indicates that the sunlight travels through the atmosphere at a path length of 1.5 times the minimum path length at the equator.) Figure 14 shows plots of the ASTM AM1.5 solar standard in (a) $\log_{10}$(W.m^{-2}.sr^{-1}.nm^{-1}) vs wavelength and (b) $\log_{10}$(photons.s^{-1}.m^{-2}.sr^{-1}.nm^{-1}) vs wavelength. In Figure 14b the plot was converted from W.m^{-2}.sr^{-1}.nm^{-1} to photons.s^{-1}.m^{-2}.sr^{-1}.nm^{-1} by dividing each value in the ASTM AM1.5 spectrum by the energy of the photon at each wavelength. The energy of a photon is $E = \frac{hc}{\lambda}$ where h is Planck's constant, c is the speed of light, and λ is the wavelength.

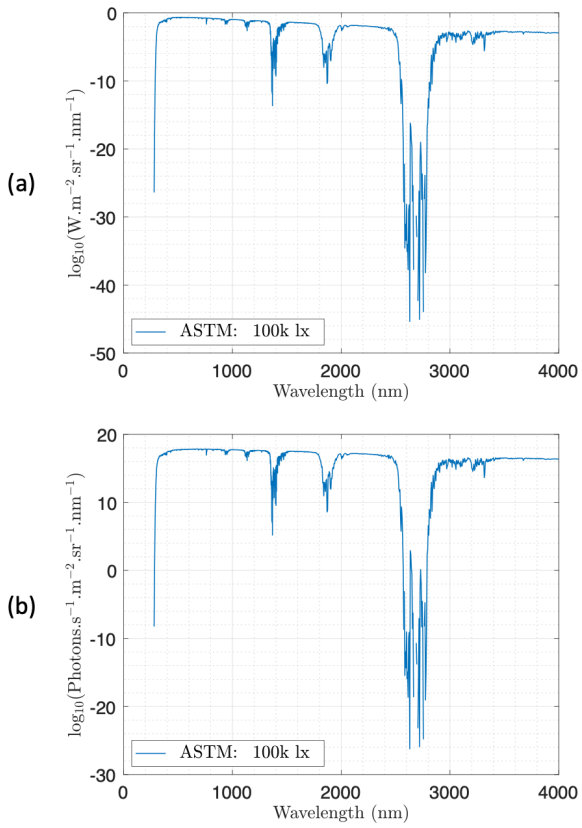


Figure 14: Plots of the ASTM AM1.5 solar standard in $\log_{10}$ scale. (a) ASTM spectrum in $\log_{10}(\mathrm{W.m^{-2}.sr^{-1}.nm^{-1}})$ vs wavelength [253] and (b) ASTM spectrum in $\log_{10}(\mathrm{photons.s^{-1}.m^{-2}.sr^{-1}.nm^{-1}})$ vs wavelength.

The peak irradiance and photon counts of the solar spectra is between 500 – 550 nm. The dips in the spectra are where the gases and molecules in the atmosphere absorb certain wavelengths and allow others to pass through. The solar atmosphere also absorbs certain wavelengths leading to Fraunhofer lines. The wavelength regions that are absorbed by atmospheric gases such as water vapour, carbon dioxide, and ozone are called atmospheric absorption bands and these cause the most attenuation [208].

Assuming the sunlight enters the room through the window and directly impinges on the entrance pupil of the receiver, the received optical power [257] is calculated by

$$P_{R,Sun} = \mathrm{A}_{det}\Omega_{det}L_{Sun} \tag{21}$$

where $P_{R,Sun}$ is the power received, A_{det} is the detector collection area, Ω_{det} is the solid angle of the detector, and L_{Sun} is the filtered sunlight radiance ($\mathrm{W.m^{-2}.sr^{-1}}$).

2.4 Initial Verification of a QKD Link Model

An indoor free-space QKD link was simulated for visible wavelengths of operation around 658 nm. A survey for comparable short range QKD experiments was also conducted. The literature review in section 1.4 reported four papers that have experimental results with practical handheld QKD systems that operated at 632 nm [132], 650 nm [133, 134], and 658 nm [55]. The parameters of the systems in these papers are shown in Table 2 and were used as representative values in simulations.

Table 2. Short range QKD link simulation parameters.

Short Range QKD Link Simulation Parameters			
	J.L. Duligall et al. 2006 [132]	D. Lowndes et al. 2021 [133, 134]	H. Chun et al. 2017 [55]
Wavelength (λ_0)	632 nm	650 nm	658 nm
Repetition rate (f_{rep})	5 MHz	80 MHz	250 MHz
Mean photon number (μ)	0.3	0.025	0.07
Pulse width (τ_{pulse})	2.17 ns	1.6 ns	1 ns
Gating window (τ)	5 ns	2 ns	1 ns
Link loss (L_L)	0 dB	10 dB	7 dB
Detector efficiency (η)	0.045	0.6	0.75 [258]
Maximum count rate per detector	36k CPS	1M CPS	1M CPS [258]
Polarisation error (p_{opt})	0.01 [29]		
Number of detectors (n)	4 [29]		

The two practical handheld QKD systems in J.L. Duligall et al. 2006 [132] and D. Lowndes et al. 2021 [133, 134] were designed and built at the University of Bristol. The QKD system reported in J.L. Duligall et al. 2006 was the first proof of principle experiment to demonstrate

a BB84 link between a handheld transmitter and receiver built from off-the-shelf components. The QKD receiver used Si APD modules (Perkin Elmer C30902S) with a 0.5 mm active diameter. The QKD system worked up to one metre in varying levels of background lighting (e.g. shaded areas but not direct sunlight) using a 5 ns gating window. The QKD system was limited by the maximum background count rate of each detector at 36k CPS.

The other QKD system reported in D. Lowndes et al. 2021 was a BB84 handheld transmitter and a receiver module inside a blackout box that simulated a Quantum ATM. The receiver module used Ø105 µm multimode fibres with NA = 0.22 (Thorlabs M43L01) attached to Si SPAD modules (Excelitas SPCM-AQ4C). The handheld QKD system worked in the presence of an artificial light source with varying levels of brightness using a 2 ns gating window. A daylight simulating alarm clock (Lumie Bodyclock Glow 150) was used to vary the background light levels from full room brightness equivalent to a well-lit room down to darkness.

The practical QKD system reported in H. Chun et al. 2017 [55] was a handheld free-space QKD system built by our Optical Wireless Communications group at the University of Oxford. The QKD system used an integrated dynamic beam steering unit at the transmitter and receiver. LED beacons, micro-electromechanical systems (MEMs) mirrors, and Position Sensing Detectors (PSDs) were used for tracking and the beam steering units successfully compensated for dynamic hand movements. The QKD receiver used fibre-coupled Si SPAD modules (ID Quantique id120 [258]). The front end of the multimode fibre is a collimator with a measured area of 5 mm^2. The handheld QKD link worked under incandescent lighting (> 400 lx) using a 1 ns gating window.

Figure 15 shows plots of the results of the QKD link simulations for the short range QKD link experiments. In the QKD link simulations, the QBER was estimated using Eq. (6) with

parameters in Table 2. The QBER is shown as a function of R_{noise} (total noise count rate per SPAD) in counts per second (CPS). Figure 15a shows the link simulations where the QBER exceeds the BB84 threshold. Figure 15b shows a subset of link simulations where the QBER exceeds the practical threshold of 4% and highlights the maximum count rate of 36k CPS for each detector used in J.L. Duligall et al. 2006.

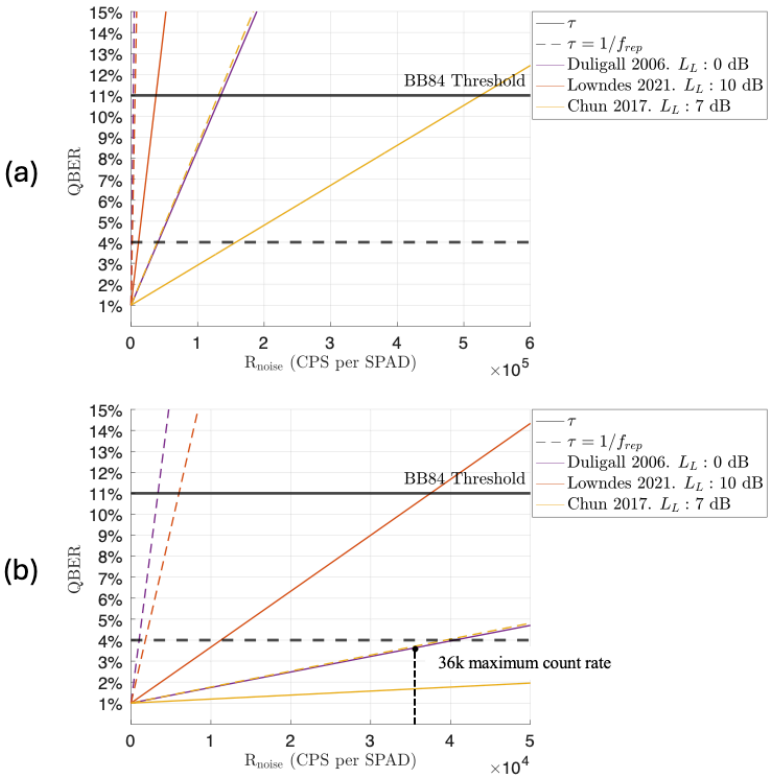


Figure 15. Plots of QBER vs total noise count rate per SPAD for the QKD link simulations for the short range QKD link experiments. Each QKD link was simulated using parameters in Table 2 for two scenarios: 1) temporal filtering with a gating window τ and 2) no temporal filtering ($\tau = \frac{1}{f_{rep}}$). The QKD links were simulated with no temporal filtering to show the minimum link tolerance for noise for each experiment. (a) The link simulations where the QBER exceeds the BB84 threshold. (b) A subset of the link simulations where the QBER exceeds the practical threshold of 4%. The maximum count rate of 36k CPS per detector used in J.L. Duligall et al. 2006 [132] is shown.

The results of the QKD link simulations show that the QKD systems of J.L. Duligall et al. 2006 and D. Lowndes et al. 2021 have a lower link tolerance for noise. The factors that limited the QKD link performance of the system in J.L. Duligall et al. 2006 are a low repetition rate (f_{rep} = 5 MHz), high mean photon number (μ = 0.3), low detection efficiency (η = 0.045), gating window larger than the pulse width ($\tau > \tau_{pulse}$), and low detector noise count rate (36k CPS per detector). The factors that limited the QKD link performance of the system in D. Lowndes et al. 2021 are a very low mean photon number (μ = 0.025) and high link loss (L_L = 10 dB). It can be seen in Figure 15a that the system in H. Chun et al. 2017 with and without temporal filtering has a much higher noise tolerance compared to the other two systems. This is mainly due to the high repetition rate (f_{rep} = 250 MHz), mean photon number (μ = 0.07), and high detection efficiency (η = 0.75). The remaining QKD link simulations in this chapter used parameters from H. Chun et. al 2017 because it has a higher noise tolerance compared to the other two systems and it was a working QKD system in our lab that was readily accessible for comparison. The ID Quantique id120 [258] SPAD module used in H. Chun et al. 2017 is a representative example of a typical silicon SPAD module.

Figure 16 shows plots of the results of the general QKD link simulations using parameters from H. Chun et al. 2017. The QBER is shown as a function of R_{noise} (total noise count rate per SPAD). Figure 16a shows the link simulations where the QBER exceeds the BB84 threshold due to the link losses (L_L). Figure 16b shows a subset of the link simulations for the QBER that exceeds the QBER = 4% practical threshold. In the link simulations, the maximum threshold for link loss is set to 14 dB. This threshold corresponds to μ = 0.1 for a realistic beam splitter attack. In the subsequent sections, the graphs of Figure 16 are used as a reference to show how well each receiver case performed under filtered LED lighting and sunlight.

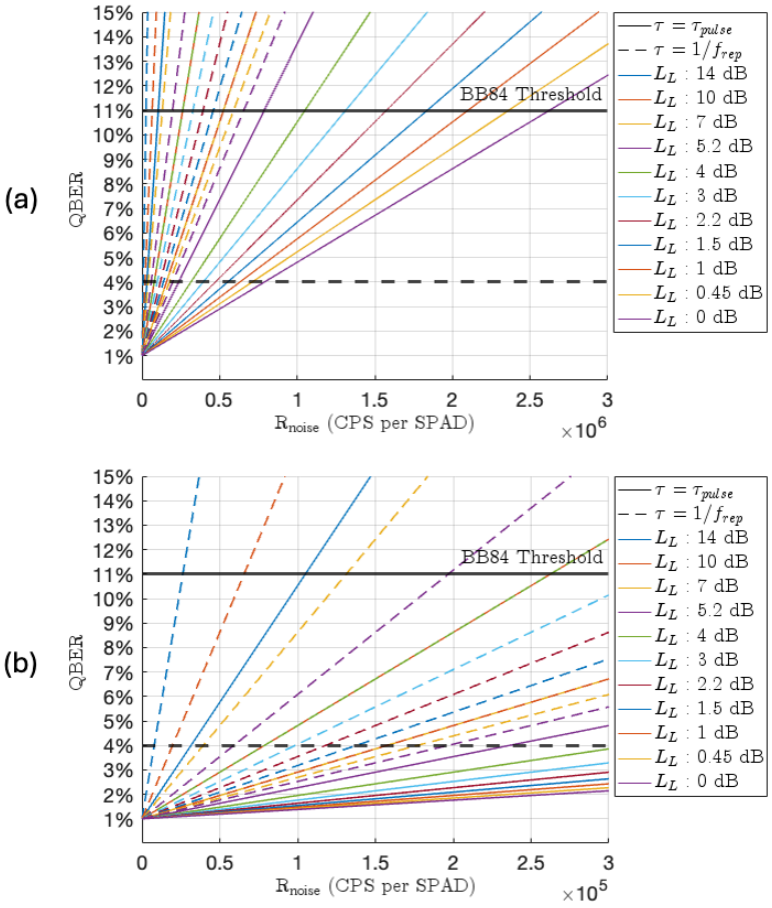


Figure 16: Plots of QBER vs total noise count rate per SPAD for QKD link simulations using parameters from H. Chun et al. 2017. The QKD links were simulated for two scenarios: 1) temporal filtering with a gating window ($\tau = \tau_{pulse} = 1$ ns) and 2) no temporal filtering ($\tau = \frac{1}{f_{rep}} = 4$ ns). No temporal filtering was used to show the minimum link tolerance for noise. The QKD links were simulated at various link losses (L_L). The maximum link loss is 14 dB which corresponds to $\mu = 0.1$ for a realistic beam splitter attack. (a) The link simulations where the QBER exceeds the BB84 threshold. (b) A subset of the link simulations where the QBER exceeds the practical threshold of 4%.

2.5 QKD Link Simulations

The QKD link simulations for the remainder of this chapter used the interference filter model, noise models, and receiver models found in Table 3. An interference filter was modelled with a 2 nm bandwidth and 95% transmittance centred at the desired wavelength. We used data from a commercially available 2 nm Alluxa Ultra Narrowband Interference Filter [259] as a model.

This was a representative example of a practical filter that was available at the wavelengths of interest. No wavelength shift was assumed due to the narrow fields of view (FOV) of the receiver. The receiver models were etendue-limited and set by two cases: 1) a receiver with a field of view of 0.1˚ and a collimator with collection area of 5 mm^2 and 2) a receiver with a single mode fibre with Ø9 μm and NA = 0.1.

Table 3: QKD link noise and receiver model parameters.

QKD Link Noise and Receiver Model Parameters	
LED model. Lambertian. Uniform illumination with average luminance of 500 lx on the desk.	$m = 1, \quad \theta = 0^{\circ}, \quad d = 3$ m, $\quad \psi = 0$ $P_{T,LED}$ = 1 W optical power (7 W total for LED lighting)
Sunlight model. Sunlight directly illuminates Rx entrance pupil.	ASTM AM1.5 spectrum at 100k lx with 90% transmittance through glass [260, 261]
Spectral filter model	2 nm bandwidth [259] centred at 658 nm and 761 nm
Receiver case 1. The detector in [55] is a fibre-coupled Si SPAD module. The front end of the multimode fibre is a collimator with a measured area of 5 mm^2.	Field of view (Ψ_c) = 0.1˚ [55] $\Omega_{det} = 2\pi(1 - \cos 0.1^{\circ})$ Collection area (A_{det}) = 5 mm^2 [55]
Receiver case 2. Etendue limited by single mode fibre (SMF).	Numerical aperture (NA) = 0.1 $\approx \Psi_c = 5.7^{\circ}$ $\Omega_{det} = 2\pi(1 - \cos 5.7^{\circ})$ Collection diameter (ØG) = 9 μm $A_{det} = \frac{\pi}{4}(9\ \mu m)^2 = 6.36 \times 10^{-5}$ mm^2

Figure 17 shows how geometrical link loss varies depending on the Airy disk beam diameter ØD and the effective area A_{eff} for the two receiver cases in Table 3. Figure 17a is a plot of geometrical link loss vs half angle FOV α for receiver case 1. Figure 17b is a plot of geometrical link loss vs half angle FOV α for receiver case 2.

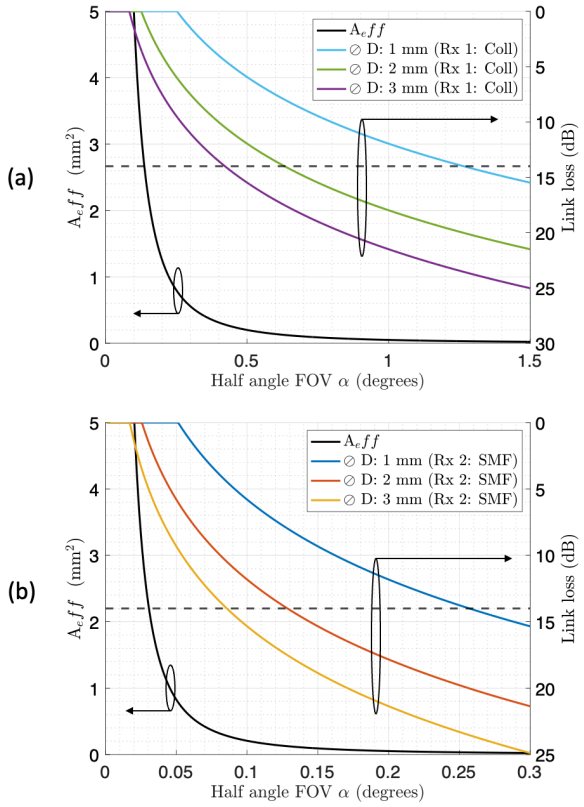


Figure 17: Plots of effective area (left y-axis) and link loss (right y-axis) vs half angle FOV of the entrance pupil for etendue-limited receiver models: (a) a receiver with a field of view of 0.1° and a collimator with collection area of 5 mm^2 and (b) a receiver with a single mode fibre. The dotted line is the maximum threshold for link loss at 14 dB. This threshold corresponds to μ = 0.1 for a realistic beam splitter attack. These plots show effectively how each receiver case can tolerate geometrical link loss while conserving the etendue.

The geometrical link loss was simulated for Airy disk diameters $\emptyset D = 1, 2, 3$ mm using Eq. (14), (15), and (17) at the receiver plane. The transmitter was directly above the receiver on the desk and the angle of incidence was set to zero $(\psi = 0)$. The detector etendue for the two receiver cases were set using the parameters found in Table 3. The effective area (A_{eff}) was varied up to 5 mm^2 and the corresponding half angle FOV of the entrance pupil (α) was set to conserve the etendue of the receiver. It can be seen in Figure 17 that an increase in the half angle FOV of the entrance pupil also decreases the effective area, and this increases the geometrical link loss. The increase in Airy disk diameter also requires an increase in the

effective area used to collect the signal. This can be seen for each Airy disk diameter in Table 4 such that an increase in the effective area decreases the half angle FOV for each receiver case at 14 dB link loss (corresponding to μ = 0.1 for a realistic beam splitter attack).

Table 4. Parameters for receiver cases 1 and 2 to conserve etendue for geometrical link loss at 14 dB.

Airy disk diameter ØD	Link loss L_L	Effective area A_{eff}	Rx Case 1 half angle FOV α	Rx Case 2 half angle FOV α
1 mm	14 dB	0.03 mm^2	1.27°	0.26°
2 mm	14 dB	0.13 mm^2	0.63°	0.13°
3 mm	14 dB	0.28 mm^2	0.42°	0.09°

In the next two sections, the QKD link simulations focused on LED lighting and sunlight around 658 nm because this was the wavelength of operation used in H. Chun et al. 2017. Figure 18 shows plots of the LED model and sunlight spectra in the visible region. Figure 18a shows the LED model spectrum converted from $W.m^{-2}.sr^{-1}.nm^{-1}$ to $photons.s^{-1}.m^{-2}.sr^{-1}.nm^{-1}$ vs wavelength. Figure 18b shows the ASTM AM1.5 spectrum at 90% transmittance through glass converted from $W.m^{-2}.sr^{-1}.nm^{-1}$ to $photons.s^{-1}.m^{-2}.sr^{-1}.nm^{-1}$ vs wavelength. In the room, it was assumed the sunlight was filtered through a glass window. Clear, transparent glass that is commercially available has an average solar transmittance of 90% [260, 261]. It can be seen in the grey highlighted region that the LED lighting and sunlight spectra are relatively high at 658 nm.

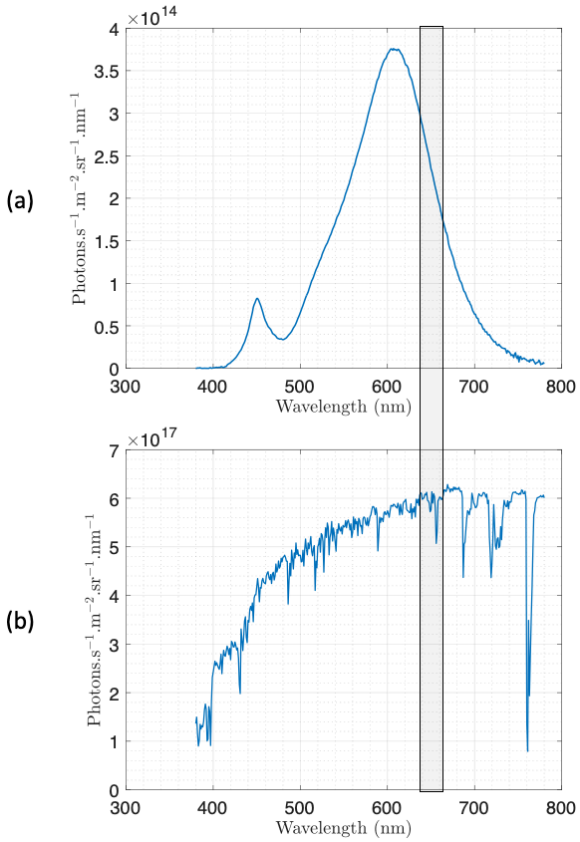


Figure 18: Plots of the LED model and sunlight spectra in the visible region around 658 nm. (a) The spectrum of the LED model in photons.s^{-1}.m^{-2}.sr^{-1}.nm^{-1} vs wavelength and (b) the sunlight spectrum in photons.s^{-1}.m^{-2}.sr^{-1}.nm^{-1} vs wavelength. The spectrum of the LED model is representative of one LED bulb at a distance of 3 metres above the desk. The sunlight spectrum is representative of sunlight at 100k lx passing through glass with 90% transmittance. The grey region is the area of interest in the QKD link simulations at 658 nm.

2.5.1 QBER Estimation in Artificial Lighting at 658 nm

An estimation was made considering only the effect of LED lighting at 658 nm. Figure 19 shows the filtered spectrum of the LED model in photons.s^{-1}.m^{-2}.sr^{-1}.nm^{-1} vs wavelength.

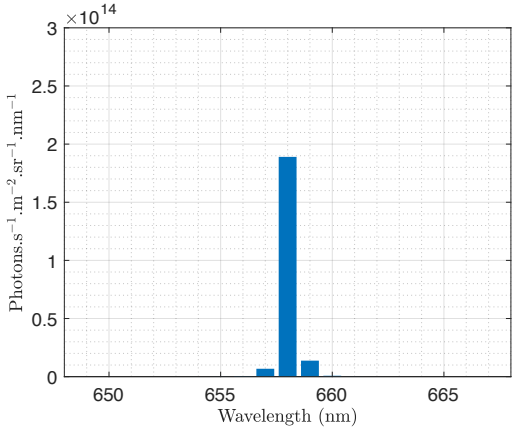


Figure 19: Plot of photons.s^{-1}.m^{-2}.sr^{-1}.nm^{-1} vs wavelength for the narrowband filtered spectrum of the LED model centred at 658 nm. The emission spectrum of the LED model from Figure 18a is filtered at 658 nm using the 2 nm commercial interference filter model. The filter model has a 95% transmittance peak at 658 nm and 1 nm spectral resolution.

The filtered spectrum of the LED model in Figure 19 was integrated across the 2 nm bandwidth of the filter and then scaled by the total number of LEDs (7) to get the total photons.s^{-1}.m^{-2}. sr^{-1} for LED lighting. (Note that the filter data available has 1 nm resolution which leads to a slight underestimation of photon flux.) The QKD link simulations were then analysed using Eq. (19) and the parameters of the LED model and the two receiver cases in Table 3. The total noise count rates for each SPAD (R_{noise}) were estimated using a model of the BB84 receiver design in Figure 9 and these are shown in Table 5. The R_{noise} in column 3 are calculated by dividing the values of total noise rate after spectral filter (PPS) in column 2 by four (corresponding to the number of detection channels) and then multiplied by 0.75 (corresponding to the PDE of the SPAD module used in H. Chun et al. 2017).

Table 5: Total noise count rate per SPAD for LED lighting filtered at 658 nm. The receiver cases are 1) a receiver with field of view of 0.1° and a collimator with collection area of 5 mm^2 and 2) a receiver with a single mode fibre with Ø9 µm and NA = 0.1.

LED Lighting Filtered at 658 nm		
Receiver cases	Total noise rate after spectral filter (PPS)	R_{noise} using $\eta = 0.75$ (CPS per SPAD)
1. Narrow FOV and collimator	141,800	26,600
2. Single mode fibre (SMF)	5,900	1,100

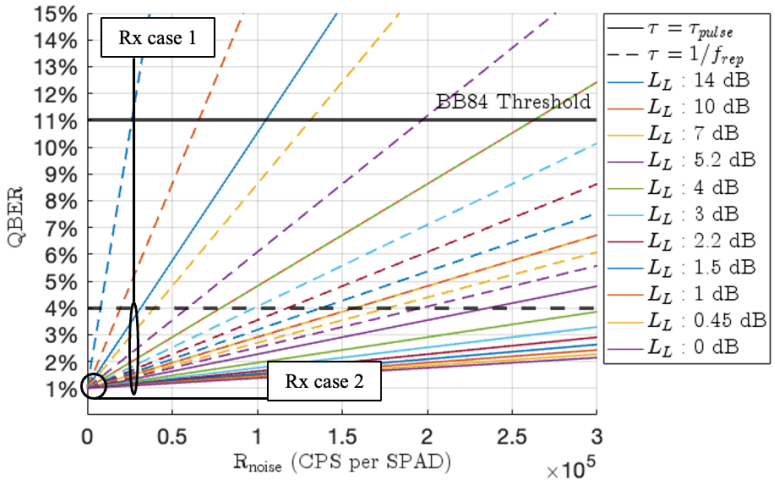


Figure 20: Plot of QBER vs total noise count rate per SPAD for the QKD link simulations under filtered LED lighting at 658 nm. The QBER is estimated for link losses ranging from 0 – 14 dB (corresponds to µ = 0.1 for a realistic beam splitter attack). The practical threshold of QBER = 4% is shown. The link losses are grouped together based on the values of R_{noise} (column 3 in Table 5) to show the feasible link parameters for the two receiver cases: 1) a receiver with a field of view of 0.1° and a collimator with collection area of 5 mm^2 and 2) a receiver with single mode fibre.

Figure 20 shows plots of the results of the QKD link simulations under filtered LED lighting at 658 nm for the two receiver cases. The simulation results suggest a QKD link operating at 658 nm can work under LED lighting. It can be seen in Figure 20 that the two receiver cases can support various link losses for the two scenarios: 1) no temporal filtering (i.e. $\tau = \frac{1}{f_{rep}} = 4$ ns) and 2) gating window around the transmit pulse width ($\tau = \tau_{pulse} = 1$ ns). Receiver case 1

(narrow FOV and collimator) can support link losses up to 7 dB below the QBER = 4% threshold and up to a maximum of 14 dB for scenario 1 (no temporal filtering). Also, receiver case 1 can support link losses up to a maximum of 14 dB for scenario 2 (gating window around the transmit pulse width). Similarly, receiver case 2 (single mode fibre) can support link losses up to a maximum of 14 dB for both scenarios because there is much less noise by restricting the half angle FOV α. The trade-off between receiver cases 1 and 2 is the FOV. In the next section, we simulate the QKD link model under sunlight.

2.5.2 QBER Estimation in Sunlight at 658 nm

An estimation was made considering only the effect of sunlight at 658 nm. The method used in this section is the same method used in section 2.3.4.2. Figure 21 shows the filtered sunlight spectrum in photons.$s^{-1}.m^{-2}.sr^{-1}.nm^{-1}$ vs wavelength.

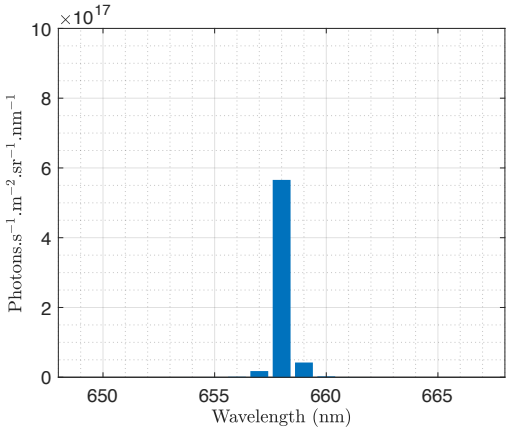


Figure 21: Plot of photons.$s^{-1}.m^{-2}.sr^{-1}.nm^{-1}$ vs wavelength for the narrowband filtered sunlight spectrum centred at 658 nm.The sunlight spectrum from Figure 18b is filtered at 658 nm using the 2 nm commercial interference filter model. The filter model has a 95% transmittance peak at 658 nm and 1 nm spectral resolution.

The filtered sunlight spectrum in Figure 21 is integrated across the 2 nm bandwidth of the filter to get the total photons.$s^{-1}.m^{-2}.\ sr^{-1}$. The QKD link simulations were then analysed using Eq. (21) and the parameters of the sunlight model and the two receiver cases in Table 3. The total

noise count rates per SPAD (R_{noise}) were estimated using the same method in section 2.5.1 for filtered LED lighting, except R_{noise} included the dark counts and sunlight and these are shown in Table 6.

Table 6: Total noise count rate per SPAD for sunlight filtered at 658 nm. The receiver cases are 1) a receiver with field of view of 0.1° and a collimator with collection area of 5 mm^2 and 2) a receiver with a single mode fibre with Ø9 µm and NA = 0.1.

Sunlight Filtered at 658 nm		
Receiver cases	Total noise rate after spectral filter (PPS)	R_{noise} using $\eta = 0.75$ (CPS per SPAD)
1. Narrow FOV and collimator	30.27×10^6	5.68×10^6
2. Single mode fibre (SMF)	1.27×10^6	2.38×10^5

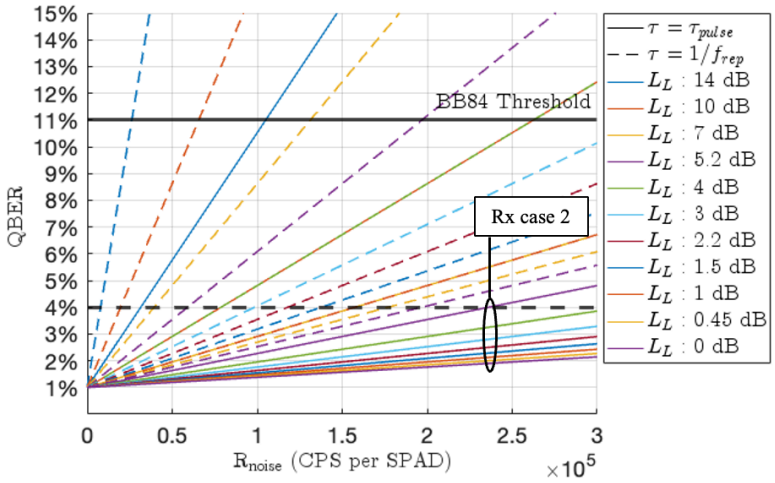


Figure 22: Plot of QBER vs total noise count rate per SPAD for the QKD link simulations under filtered sunlight at 658 nm. The QBER is estimated for link losses ranging from 0 – 14 dB (corresponds to µ = 0.1 for a realistic beam splitter attack). The practical threshold of QBER = 4% is shown. The link losses that are grouped together based on the values of R_{noise} (column 3 in Table 6) are only shown for receiver case 2 (single mode fibre).

Figure 22 shows a plot of the results of the QKD link simulations under direct sunlight at 658 nm for receiver case 2 (single mode fibre) only. Receiver case 1 (narrow FOV and collimator), even with no link loss, is not shown because the large number of photon counts (5.68×10^6

CPS) would result in a QBER > 11% as can be seen in Figure 16a. The simulation results suggest a QKD link operating at 658 nm could work in sunlight for receiver case 2 depending on the gating window used and the link loss of the QKD system. It can be seen in Figure 22 that only receiver case 2 can support various link losses for the two scenarios: 1) no temporal filtering (i.e. $\tau = \frac{1}{f_{rep}} = 4$ ns) and 2) gating window around the transmit pulse width ($\tau = \tau_{pulse} = 1$ ns). Receiver case 2 can support a maximum link loss of 4 dB for scenario 1 (no temporal filtering). This is less than the link loss of 7 dB in the QKD system reported in H. Chun et al. [55]. Similarly, receiver case 2 can support link losses up to 5.2 dB below the QBER = 4% threshold and up to a maximum of 10 dB for scenario 2 (gating window around the transmit pulse width).

In order to verify the QKD link simulation, we compared the simulation results in this section with the results of the free-space QKD link in [116] which operated at a wavelength close to 670 nm. In the experimental setup in [116], the QKD transmitter operated with an average mean photon number between 0.1 – 0.13. The QKD receiver used a Catadioptric reflecting telescope (focal length 500 mm) for collection, 10 nm bandwidth interference filter, and used a spatial filter to further reduce background counts with a 75 μm diameter pinhole and optics that narrowed the field of view. The receiver etendue is unknown. The interference filter was chosen to have 10 nm bandwidth due to the angular subtense from the reflecting light into the receiver optics. Narrower filters would not be able to capture the light from all angles of the reflector surface through the pinhole. The detectors are Si SPAD modules that operated in gated mode with a 1.5 ns gating window. Although the PDE per detector was unknown, each detector had a typical dark count rate of 750 CPS. The receiver configurations for the 658 nm and 670 nm links are completely different and cannot be directly compared. Similarly, the artificial lighting and daylight conditions are different and cannot be directly compared. However, it is possible

to compare the two links based only on the number of photon counts at each detector from the ambient light scenarios.

In [116] the free-space QKD link worked in darkness and subdued fluorescent lighting in the laboratory with background counts of 1×10^4 CPS. For this level of photon counts at each SPAD module, the simulation results in Figure 20 are consistent with the experimental results in [116]. It is clear that the 658 nm and 670 nm QKD links work indoors and under artificial lighting. In [116] the free-space QKD link also worked in daylight under cloudy conditions. The lux level of the scenario is unknown; hence, this lux level must be inferred. A typical lux level for daylight under cloudy skies is 30k lx. In comparison, the sunlight model in Figure 18 uses a solar spectrum at 100k lx with 90% transmittance through glass. Consequently, the number of photons per second at 658 nm in sunlight that are already filtered in Table 6 can effectively be 1/3 of the photon count rate. In Figure 22 if R_{noise} is less than 1/3 of the count rate (i.e. decrease from 2.38×10^5 CPS to 7.93×10^4 CPS), the QKD link will work for receiver case 2 that uses the single mode fibre. The experiment in [116] had an average QBER around 5%. The QKD link could work for link losses up to 10 dB at QBER = 5% and 14 dB maximum for scenario 2 (gating window around the transmit pulse width). Therefore, the results of the 658 nm simulation agree with the experimental results in [116] when considering only the photon count rate affecting the QBER.

2.6 Line Of Sight QKD Link Simulation at 761 nm

The results of the QKD link simulations in the previous section indicate the QKD link at 658 nm works under LED lighting and for certain conditions for a receiver using a single mode fibre under sunlight. Based on the significant drop in the number of photons at 761 nm, another QKD link simulation was undertaken. The drop is caused by the Oxygen A absorption band and a QKD link operating in this band offers a means to reduce the effect of LED lighting and sunlight and still use silicon detectors. The rest of this section follows the same methods for the simulations under LED lighting and sunlight as shown in sections 2.5.1 and 2.5.2 respectively.

Figure 23 shows plots of the LED model and sunlight spectra in the visible region. Figure 23a shows the LED model spectrum converted from $W.m^{-2}.sr^{-1}.nm^{-1}$ to $photons.s^{-1}.m^{-2}.sr^{-1}.nm^{-1}$ vs wavelength. Figure 23b shows the ASTM AM1.5 spectrum at 90% transmittance through glass converted from $W.m^{-2}.sr^{-1}.nm^{-1}$ to $photons.s^{-1}.m^{-2}.sr^{-1}.nm^{-1}$ vs wavelength. It can be seen in the grey highlighted region that the LED lighting at 761 nm is less than 5% relative to 658 nm. Similarly, the sunlight spectra at 761 nm is less than 17.5% relative to 658 nm.

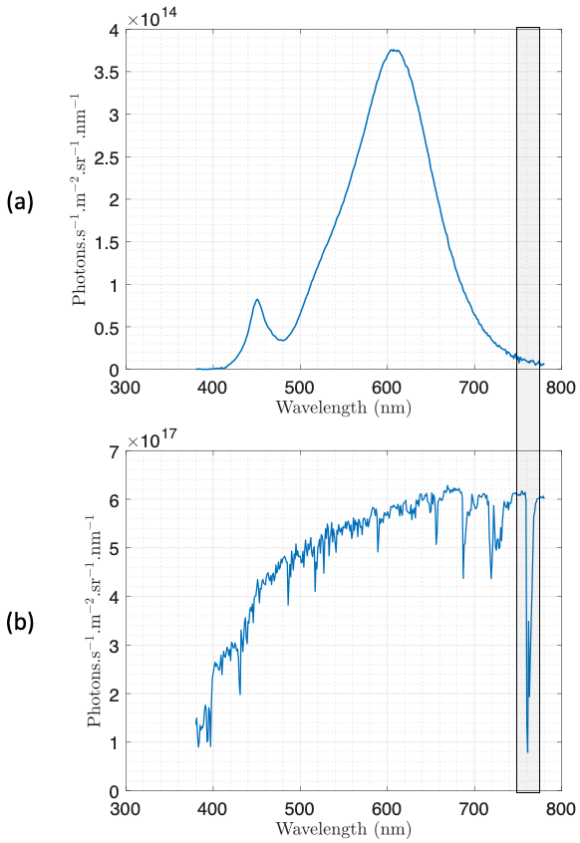


Figure 23: Plots of the LED model and sunlight spectra in the visible region around 761 nm.(a) The spectrum of the LED model in photons.s^{-1}.m^{-2}.sr^{-1}.nm^{-1} vs wavelength and (b) the sunlight spectrum in photons.s^{-1}.m^{-2}.sr^{-1}.nm^{-1} vs wavelength. The spectrum of the LED model is representative of one LED bulb at a distance of 3 metres above the desk. The sunlight spectrum is representative of sunlight at 100k lx passing through glass with 90% transmittance. The grey region is the area of interest in the QKD link simulations at 761 nm.

Figure 24 shows a zoomed-in plot of the sunlight spectrum with the region of interest around 761 nm. The graph shows the two wavelengths where there are the lowest number of photons in the Oxygen A absorption band are at 760 and 761 nm.

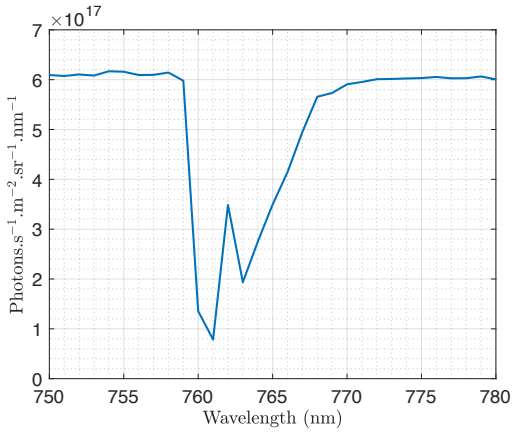


Figure 24: Plot of photons.s^{-1}.m^{-2}.sr^{-1}.nm^{-1} vs wavelength for the zoomed-in narrowband sunlight spectrum around 761 nm.The narrowband dip in the spectrum is caused by the Oxygen A absorption band.

2.6.1 QBER Estimation in Artificial Lighting at 761 nm

An estimation was made considering only the effect of LED lighting at 761 nm, similar to the QBER estimation in section 2.5.1. The total noise count rates for each SPAD (R_{noise}) are shown in Table 7. The total noise count rates at 761 nm in Table 7 are less than 5% of the total noise count rates at 658 nm in Table 5.

Table 7: Total noise count rate per SPAD for LED lighting filtered at 761 nm. The receiver cases are 1) a receiver with field of view of 0.1° and a collimator with collection area of 5 mm^2 and 2) a receiver with a single mode fibre with Ø9 µm and NA = 0.1.

LED Lighting Filtered at 761 nm		
Receiver cases	Total noise rate after spectral filter (PPS)	R_{noise} using η = 0.75 (CPS per SPAD)
1. Narrow FOV and collimator	6,570	1,230
2. Single mode fibre (SMF)	270	51

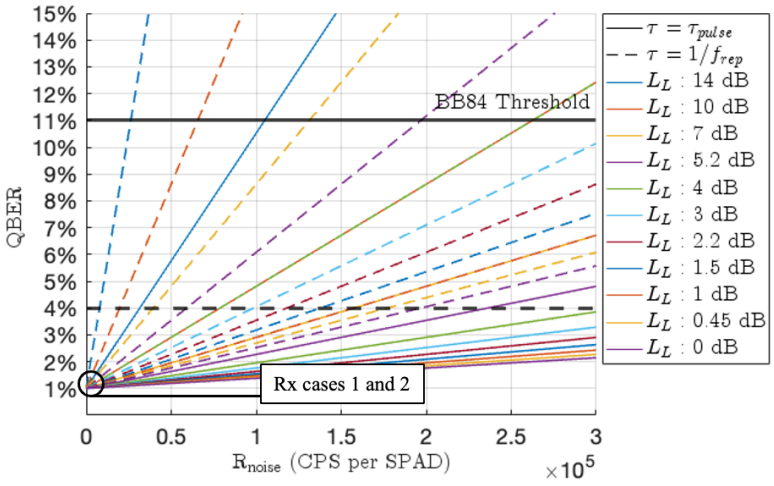


Figure 25: Plot of QBER vs total noise count rate per SPAD for the QKD link simulations under filtered LED lighting at 761 nm. The QBER is estimated for link losses ranging from 0 – 14 dB (corresponds to $\mu = 0.1$ for a realistic beam splitter attack). The practical threshold of QBER = 4% is shown. The link losses are grouped together based on the values of R_{noise} (column 3 in Table 7) to show the feasible link parameters for the two receiver cases: 1) a receiver with a field of view of 0.1° and a collimator with collection area of 5 mm^2 and 2) a receiver with a single mode fibre.

Figure 25 shows plots of the results of the QKD link simulations under filtered LED lighting at 761 nm for the two receiver cases. It can be seen in Figure 25 that the noise count rates and QBER are extremely low such that a QKD link at 761 nm can work under LED lighting. This QKD link works for both receiver cases, with and without temporal filtering, and up to a maximum link loss of 14 dB.

2.6.2 QBER Estimation in Sunlight at 761 nm

An estimation was made considering only the effect of sunlight at 761 nm, similar to the QBER estimation in section 2.5.2. Figure 26 shows the filtered sunlight spectrum in photons.s^{-1}.m^{-2}.sr^{-1}.nm^{-1} vs wavelength.

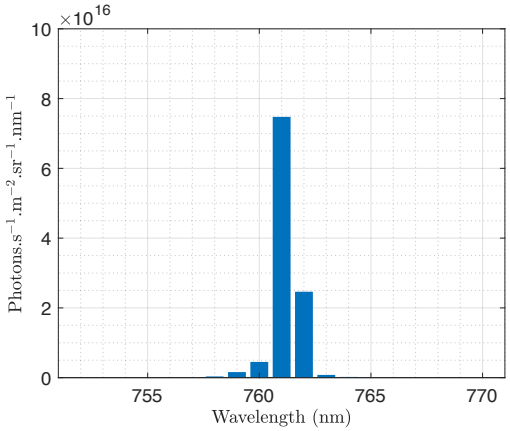


Figure 26: Plot of photons.s^{-1}.m^{-2}.sr^{-1}.nm^{-1} vs wavelength for the narrowband filtered sunlight spectrum centred at 761 nm.The sunlight spectrum from Figure 23b is filtered at 761 nm using the 2 nm commercial interference filter model. The filter model has a 95% transmittance peak at 761 nm and 1 nm spectral resolution.

The total noise count rates for each SPAD (R_{noise}) are shown in Table 8. The total noise count rates under sunlight at 761 nm in Table 8 are less than 17.5% of the total noise count rates at 658 nm in Table 6.

Table 8: Total noise count rate per SPAD for sunlight filtered at 761 nm. The receiver cases are 1) a receiver with field of view of 0.1° and a collimator with collection area of 5 mm^2 and 2) a receiver with a single mode fibre with Ø9 µm and NA = 0.1.

Sunlight Filtered at 761 nm		
Receiver cases	Total noise rate after spectral filter (PPS)	R_{noise} using η = 0.75 (CPS per SPAD)
1. Narrow FOV and collimator	5.26×10^6	9.86×10^5
2. Single mode fibre	217,000	40,700

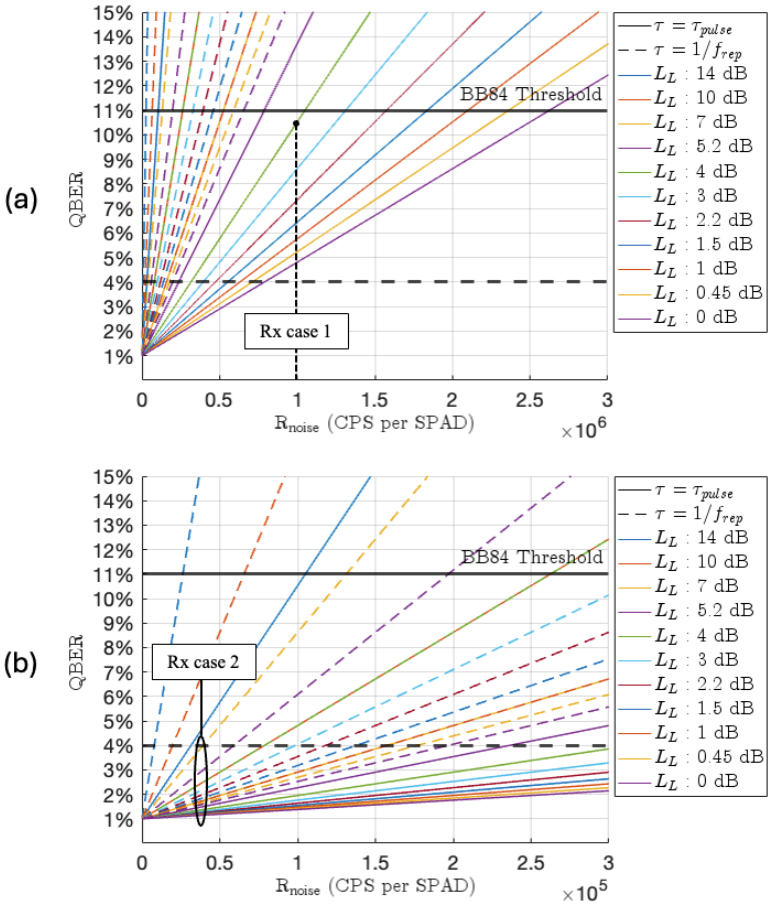


Figure 27: Plot of QBER vs total noise count rate per SPAD for the QKD link simulations under filtered sunlight at 761 nm. The QBER is estimated for link losses ranging from 0 – 14 dB (corresponds to μ = 0.1 for a realistic beam splitter attack). The practical threshold of QBER = 4% is shown. The link losses that are grouped together based on the values of R_{noise} (column 3 in Table 8) to show the feasible link parameters for the two receiver cases: 1) a receiver with a field of view of 0.1° and a collimator with collection area of 5 mm^2 and 2) a receiver with single mode fibre.

Figure 27 shows plots of the results of the QKD link simulations under direct sunlight at 761 nm for the two receiver cases. Receiver case 1 (narrow FOV and collimator), even with a gating window around the transmit pulse width, does not work because the large number of photon counts (9.86×10^5 CPS) would nearly saturate a SPAD with a maximum count rate of 1M CPS [258]. The simulation results suggest a QKD link operating at 761 nm can work in sunlight for a single mode fibre. It can be seen in Figure 27 that only receiver case 2 (single mode fibre) can support various link losses for the two scenarios: 1) no temporal filtering (i.e. $\tau = \frac{1}{f_{rep}} = 4$

ns) and 2) gating window around the transmit pulse width ($\tau = \tau_{pulse} = 1$ ns). Receiver case 2 can support a link loss of up to 7 dB at QBER = 4% and up to a maximum link loss of 10 dB for scenario 1 (no temporal filtering). Receiver case 2 can support link losses up to 10 dB below the QBER = 4% threshold and up to a maximum of 14 dB for scenario 2 (gating window around the transmit pulse width).

2.7 Discussions and Observations

Table 9. Results summary of the QKD link simulations at 658 nm.

Results Summary of the QKD Link Simulations at 658 nm		
Receiver cases	(1) Narrow FOV and collimator	(2) SMF
LED lighting – 500 lx R_{noise} using $\eta = 0.75$ (CPS per SPAD)	26,600	1,100
	Maximum link loss tolerance (dB)	
$\tau = \tau_{pulse} = 1$ ns	14	14
$\tau = \frac{1}{f_{rep}} = 4$ ns	14	14
	Link loss tolerance at QBER = 4% (dB)	
$\tau = \tau_{pulse} = 1$ ns	14	14
$\tau = \frac{1}{f_{rep}} = 4$ ns	7	14
QKD link works under LED lighting? ($L_L = 7$ dB threshold)	Yes	Yes
Sunlight – 90k lx R_{noise} using $\eta = 0.75$ (CPS per SPAD)	5.68×10^6	2.38×10^5
	Maximum link loss tolerance (dB)	
$\tau = \tau_{pulse} = 1$ ns	n/a	10
$\tau = \frac{1}{f_{rep}} = 4$ ns	n/a	4
	Link loss tolerance at QBER = 4% (dB)	
$\tau = \tau_{pulse} = 1$ ns	n/a	5.2
$\tau = \frac{1}{f_{rep}} = 4$ ns	n/a	n/a
QKD link works under sunlight? ($L_L = 7$ dB threshold)	No	Yes (gating only)

Table 10. Results summary of the QKD link simulations at 761 nm.

Results Summary of the QKD Link Simulations at 761 nm		
Receiver cases	(1) Narrow FOV and collimator	(2) SMF
LED lighting – 500 lx R_{noise} using $\eta = 0.75$ (CPS per SPAD)	1,230	51
	Maximum link loss tolerance (dB)	
$\tau = \tau_{pulse} = 1$ ns	14	14
$\tau = \frac{1}{f_{rep}} = 4$ ns	14	14
	Link loss tolerance at QBER = 4% (dB)	
$\tau = \tau_{pulse} = 1$ ns	14	14
$\tau = \frac{1}{f_{rep}} = 4$ ns	14	14
QKD link works under LED lighting? ($L_L = 7$ dB threshold)	Yes	Yes
Sunlight – 90k lx R_{noise} using $\eta = 0.75$ (CPS per SPAD)	9.86×10^5	40,700
	Maximum link loss tolerance (dB)	
$\tau = \tau_{pulse} = 1$ ns	4	14
$\tau = \frac{1}{f_{rep}} = 4$ ns	n/a	10
	Link loss tolerance at QBER = 4% (dB)	
$\tau = \tau_{pulse} = 1$ ns	n/a	10
$\tau = \frac{1}{f_{rep}} = 4$ ns	n/a	7
QKD link works under sunlight? ($L_L = 7$ dB threshold)	No	Yes

Table 9 and Table 10 shows a summary of the results for the QKD link simulations for the wavelengths of operation at 658 and 761 nm respectively. The maximum link loss of 7 dB was reported in [55] and this threshold was used to assess the QKD link simulations in Table 2. The LED lighting has minimal effect on the QKD link for the two receiver cases. As expected, the QKD link receiver case with the single mode fibre in combination with a gating window around the pulse width greatly reduced the amount of ambient light onto the detector across all of the

simulations. The preliminary modelling showed that operating a QKD link at 658 nm can only work in sunlight when the receiver uses a single mode fibre. It can be seen in Table 9 that the QKD link at 658 nm under sunlight using receiver case 2 (single mode fibre) has a maximum allowed link loss of 10 dB. However, the QKD link simulation result in Figure 22 shows the QBER = 10% for a link loss of 10 dB. This results in a link margin of 1% for error correction and privacy amplification. The link margin is the difference between the expected QBER and the maximum QBER (e.g. 11% in the BB84 protocol). The parameters would be difficult to achieve for this QKD link to work.

Similarly, the QKD link at 761 nm can potentially work in sunlight when the receiver uses a single mode fibre. However, it can be seen in Table 10 that the 40,700 noise count rate due to sunlight is still relatively high for a typical SPAD. This can lead to an increase in QBER and decrease the link margins. The narrow nature of the Oxygen A absorption band, as shown in Figure 24, requires a narrowband spectral filter which limits the field of view of a QKD receiver. Furthermore, such a spectral filter is typically expensive [248]. These are the primary reasons 761 nm is not a practical operational wavelength for an indoor free-space QKD link.

2.8 Summary

In this chapter, a model was developed to simulate the effect of ambient light on a QKD receiver and its effects on an indoor free-space QKD link were assessed. The components of the indoor QKD link model such as the transmitter, receiver, link loss, and noise sources (LED lighting and sunlight) were described in detail. The QKD links were simulated for two wavelengths of operation in the visible spectrum (658 and 761 nm) in the presence of two sources of ambient light (LED lighting and sunlight). The wavelength of 761 nm was chosen because it had the

lowest photon counts in the visible spectrum. This reduction in photon counts is caused by the Oxygen A absorption band.

The results of the QKD link simulations showed that, with a 2 nm interference filter, both wavelengths of operation worked under LED lighting regardless of using a gating window. The wavelength of operation at 658 nm only worked under sunlight with a single mode fibre at the QKD receiver using a 1 ns gating window. This link could tolerate a maximum link loss of 10 dB. The wavelength of operation at 761 nm worked under sunlight with a single mode fibre at the QKD receiver regardless of using a gating window. This link could tolerate a maximum link loss of 14 dB. However, the narrow nature of the Oxygen A absorption band required a narrowband spectral filter. This limited the field of view of the QKD receiver and such a filter was typically expensive. These were the primary reasons 761 nm was not a practical operational wavelength for an indoor free-space QKD link. Wavelength regions where there is minimal solar irradiance are potential novel regions to explore for free-space QKD. The atmospheric absorption bands have potential use for QKD links due to the low number of photons within the bands. The next chapter investigates a new spectral region that has not been used for QKD and shows significant improvement in QBER.

Chapter 3 Solar Measurements and Link Simulation at 1370 nm

In this chapter, we investigate the use of 1370 nm radiation to operate a QKD link. We perform a series of measurements to characterise the effect of solar radiation on a typical photon-counting detector as would be used in a QKD system, and the influence of this ambient light on the QKD link performance is investigated.

3.1 The use of 1370 nm in QKD links

While it is possible to use an atmospheric absorption band at 761 nm as investigated in the previous chapter, there is a wider atmospheric absorption band at 1370 nm that can potentially be used. Figure 28 shows plots of the ASTM AM1.5 spectrum. Figure 28a is a plot of the ASTM AM1.5 spectrum in photons.s^{-1}.m^{-2}.nm^{-1} vs wavelength. The primary region of interest that is highlighted in the box is the water and carbon dioxide absorption band [208]. Figure 28b is a plot of the $\log_{10}$(photons.s^{-1}.m^{-2}.nm^{-1}) vs wavelength from 1351 – 1414 nm.

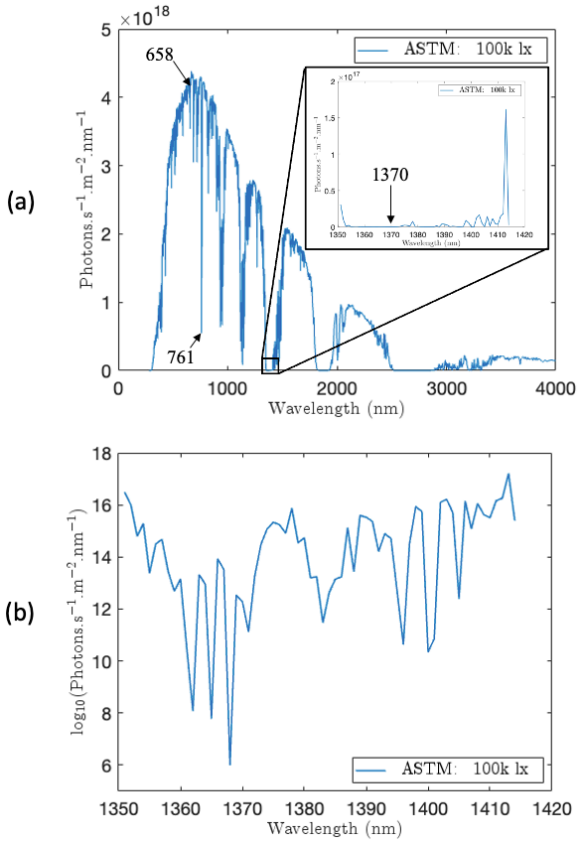


Figure 28: Plots of the ASTM AM1.5 spectrum between 1351 – 1414 nm. (a) Plot of ASTM AM1.5 spectrum in photons.s^{-1}.m^{-2}.nm^{-1} vs wavelength and (b) plot of ASTM AM1.5 spectrum in $\log_{10}$(photons.s^{-1}.m^{-2}.nm^{-1}) vs wavelength between 1351 – 1414 nm.

It can be seen in Figure 28b that a narrowband region around 1370 nm has the lowest number of photon counts in this band and is orders of magnitude lower than the photon counts at 761 nm. This shows the promise of this region. Figure 28a shows the region is relatively flat which allows a more practical wideband filter to be used. A larger bandwidth filter can improve performance by increasing the field of view at the receiver to allow for mobility and ease of alignment. It can also reduce the cost to a QKD system as manufacturers can produce such filters at lower cost. There is the additional benefit that LEDs do not operate in this absorption band. Effectively, LED lighting does not contribute noise to a QKD link that operates around 1370 nm. In the next section, we report the results of a set of experiments designed to characterise the effect of ambient light on a typical photon-counting detector as would be used in a QKD system operating in this region.

3.2 Ambient Light Measurements

The experiments were designed to estimate the photon counts per second (CPS) induced by outdoor and indoor ambient light and the potential effect on a typical QKD receiver in the 1351 – 1414 nm region. Figure 29 shows the experimental apparatus. The experimental apparatus consisted of a calibrated NIR Flame spectrometer (6 nm resolution) with a Ø600 µm fibre and cosine corrector (Ocean Insight FLAME-NIR-INTSMA25) used to measure the spectrum. A SPAD module (ID Quantique idQube low-noise model [243]) with a single mode fibre input was used to count photons. An Amprobe LM-100 lux meter was used to measure the lux levels. The fibre inputs of the spectrometer and the SPAD module were fixed on a post that directed them towards the same source. At the front end of the single mode fibre was a 10 nm passband filter centred at 1370 nm (Spectrogon NB-1370-010 [262]) and collimator with Ø6 mm aperture (Thorlabs F280FC-C).



(a) (b) (c)

Figure 29: Experimental apparatus for ambient light experiment using spectrometer and SPAD module. The experimental apparatus was used to measure photon counts per second, the spectrum, and lux levels in three sets of experiments: (a) outside under clear skies at 100k lx in direct sunlight, (b) outside under cloudy skies at 30k lx, (c) inside a meeting room at 12k lx.

Four measurements were made. The experimental apparatus was used in four sets of experiments: a) on a terrace outside a meeting room under clear skies (100k lx), b) under cloudy skies (30k lx), c) inside a meeting room (12k lx), and d) inside a laboratory with LED ceiling lighting only. In order to estimate the ambient level of the LED, the experimental apparatus was placed against the ceiling light. The measured illuminance was 100k lx.

The spectrometer had a cosine corrector attached to the front end of the fibre. A cosine corrector is an optical diffuser that increases the field of view of the fibre up to 180˚ (2π steradians). The advantages of a cosine corrector are improved sampling geometry and improved stability as the spectral measurements are angle dependent. The SPAD module was configured for free-running mode. The dead time was set to 25 μs. The PDE of the SPAD module could be set to 10, 15, 20, and 25% by adjusting the bias voltage. The PDE is a function of wavelength and the PDE was 12% at 1370 nm for the low bias voltage setting of this SPAD module (see section 2.3.2.1 Figure 8 for detailed diagrams taken from the idQube datasheet [243]). Thus, the PDE of the SPAD module was set to 10%. Consequently, the measured dark count rate was 500 CPS on average. The lux meter was used as a photometric reference. Lux is a measure of the intensity of light as perceived by human eyes. One lux is defined as one lumen per square metre ($lm.m^{-2}$) where one lumen is the total quantity of visible light emitted by a source. The lux has a corresponding radiometric unit which is one watt per square metre ($W.m^{-2}$). The difference between the two units is the radiometric unit ($W.m^{-2}$) is a physical quantity and equally weighted across all wavelengths. The photometric unit (lux) is based on the sensitivity of the human eye to different wavelengths in the visible spectrum. This sensitivity is represented by a luminous efficiency function that resembles a normal distribution with a peak at the green wavelengths (brightest) and the blue and red wavelengths are lower at the tails (weakest) [263]. The lux measurements ensured the experiments were repeatable with reproducible results.

Figure 30 shows plots of the measured spectra captured by the NIR Flame spectrometer in $\log_{10}(\text{photons.s}^{-1}.\text{m}^{-2}.\text{nm}^{-1})$ vs wavelength and the ASTM AM1.5 spectrum for reference. Figure 30a shows a plot of the measured spectra for all four experiments for the bandwidth of the spectrometer in $\log_{10}(\text{photons.s}^{-1}.\text{m}^{-2}.\text{nm}^{-1})$ vs wavelength. Figure 30b shows a plot of the measured spectra for all four experiments from 1351 – 1414 nm in $\log_{10}(\text{photons.s}^{-1}.\text{m}^{-2}.\text{nm}^{-1})$ vs wavelength.

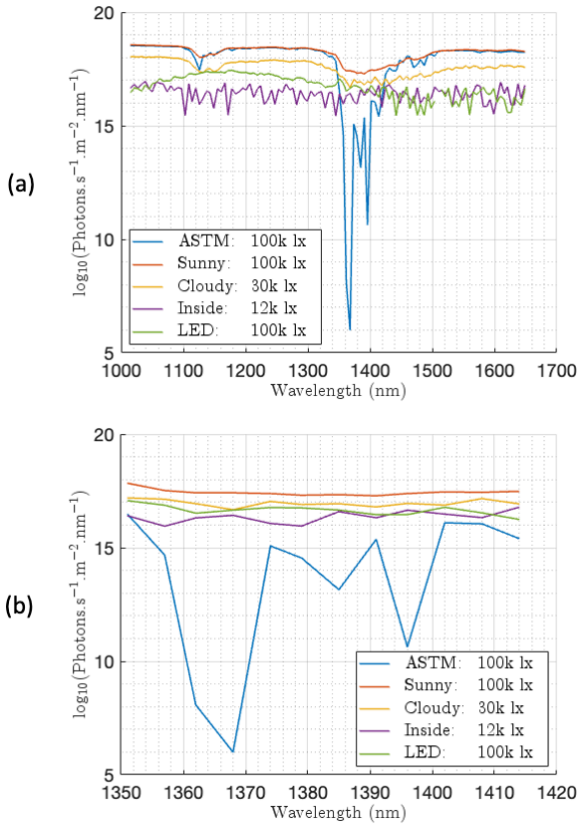


Figure 30: Plots of the measured ambient light spectra captured by the NIR Flame spectrometer. (a) Plot of measured spectra by the NIR Flame spectrometer in $\log_{10}(\text{photons.s}^{-1}.\text{m}^{-2}.\text{nm}^{-1})$ vs wavelength and (b) plot of measured spectra from 1351 – 1414 nm region in $\log_{10}(\text{photons.s}^{-1}.\text{m}^{-2}.\text{nm}^{-1})$ vs wavelength. The plots show the measured spectra for the three sets of experiments in Figure 29 and the measured spectrum under LED ceiling lighting in a laboratory. The ASTM AM1.5 spectrum at 100k lx is plotted as a reference alongside the measured spectra.

The measured spectra shown in Figure 30 were from the three sets of experiments in Figure 29 and the spectrum measured under LED ceiling lighting in a laboratory. The noise floor of the

spectrometer was measured in a dark room prior to the experiments. Each of the measured spectra have the noise floor removed. The spectrometer was calibrated by the manufacturer for irradiance ($W.m^{-2}$) over a bandwidth of 1015 – 1654 nm with a cosine corrector that had 2π steradians FOV. The spectra were converted from $W.m^{-2}.nm^{-1}$ to $photons.s^{-1}.m^{-2}.nm^{-1}$. The next two sections describe the two methodologies for estimating the photon counts using 1) the measured spectra from the spectrometer and 2) the angular FOV of the collimator.

3.2.1 Method 1 – Estimation Using Measured Spectra

The photon counts were estimated for three wavelength ranges using the measured spectra. The three wavelength ranges were 1) the bandwidth of the spectrometer (1015 – 1654 nm), 2) the region of interest (1351 – 1414 nm), and 3) the 10 nm passband of the Spectrogon filter (1367 – 1377 nm). The PDE of the SPAD module was set to 10% detection efficiency and it was assumed that 10% detection efficiency was the same across all wavelengths. This was a reasonable assumption because the PDE of the SPAD module ranged from 10 – 12% between 1351 – 1414 nm (see section 2.3.2.1 Figure 8). The photon count estimates were achieved by multiplying the unfiltered measured spectra in Figure 30 with the 10% photon detection efficiency across all wavelengths. Next, the spectra were multiplied by $1/2\pi$ steradians to remove the cosine corrector field of view. Then the spectra were multiplied by the etendue of the SPAD module which consisted of a Ø9 µm single mode fibre with numerical aperture of 0.1. Finally, the resultant spectra in $photon\ counts.s^{-1}.nm^{-1}$ vs wavelength were multiplied with the transmittance values found in the Spectrogon 10 nm passband filter datasheet for wavelengths 1015 – 1654 nm and integrated across the three wavelength ranges to estimate the total photon counts per second (CPS). The estimated results are in Table 11 in section 3.2.3.

In this thesis, a general formula for etendue ($A_{det}\Omega_{det}$) was described in Eq. (14) from chapter 2 section 2.3.2 to model and simulate two types of receiver cases. This general formula for etendue was used in method 1 (section 3.2.1). An improvement to the single mode fibre receiver model is to use the mode field diameter (MFD) instead of the core diameter of the fibre. In an optical fibre the field of view is represented by the acceptance angle or numerical aperture (NA) of the fibre. The small angle approximation for the detector solid angle is $\Omega'_{det} = \pi(NA)^2 = \pi(n\sin\theta)^2 \approx \pi\theta^2$ where θ is the half angle of the acceptance aperture in radians and n = 1 in free space. The area A'_{det} is the cross-sectional area of the fibre end and the MFD is more representative of the amount of light collected in a single mode fibre. The irradiance distribution across a single mode fibre can be modelled as a Gaussian curve with the intensity peak at the centre of the core and dropping off at $\frac{1}{e^2}$ into the cladding. This is typical of a stepped-index fibre where most of the energy is confined to the core and evanescent waves penetrate into the cladding. Hence, $A'_{det} = \frac{\pi}{4}(MFD)^2$. The equations for acceptance angle θ_{SM} and MFD are found in [264]. The MFD depends on the number of propagating modes in a fibre denoted as the V-number [220].

$$V_{number} = \frac{\pi 2a(NA)}{\lambda_0} \tag{22}$$

$$MFD = 2\omega = 2a\left(0.65 + \frac{1.619}{(V_{number})^{\frac{3}{2}}} + \frac{2.879}{(V_{number})^6}\right) \tag{23}$$

$$\theta_{SM} = \frac{\lambda_0}{\pi\left(\frac{MFD}{2}\right)} \tag{24}$$

where V_{number} is the V-number, a is the radius of the fibre core, NA is the numerical aperture of the fibre, λ_0 is the vacuum wavelength of the radiant energy, MFD is the mode field diameter, ω is the Gaussian beam waist, and θ_{SM} is the half angle of acceptance for the single mode fibre.

Eq. (22) – (24) are calculated with the same parameters ($\lambda_0 = 1370$ nm, $NA = 0.1$, $a = 4.5$ μm) from the etendue calculation used for method 1. The equations yield: $V_{number} = 2.06$,

$MFD = 11.1$ µm, and $\theta_{SM} = 78.57 \times 10^{-3}$ radians. The new solid angle is calculated as $\Omega'_{det} = \pi(\theta_{SM})^2 = 19.39 \times 10^{-3}$ radians which is smaller than $\Omega_{det} = \pi NA^2 = 31.41 \times 10^{-3}$ radians. The detector area is $A'_{det} = \frac{\pi}{4}(MFD)^2 = 96.76 \times 10^{-12}$ m^2 which is larger than $A_{det} = \frac{\pi}{4}(\emptyset 9\mu m)^2 = 63.61 \times 10^{-12}$ m^2. Consequently, the two etendue calculations show that $A_{det}\Omega_{det} = 2 \times 10^{-12}$ m^2.sr is larger than $A'_{det}\Omega'_{det} = 1.87 \times 10^{-12}$ m^2.sr. Hence, in this thesis the general equation for etendue ($A_{det}\Omega_{det}$) from chapter 2 section 2.3.2 slightly overestimates the photon counts due to sunlight by 6.6%.

3.2.2 Method 2 – Estimation Using Angular FOV of Collimator

The number of photon counts from sunlight received by the SPAD module in the experimental apparatus were estimated by approximating the etendue between the collimator and the Sun. It is assumed the collimator points directly at the Sun. The FOV of the collimator with respect to the Sun is calculated from a ratio of the solid angles for the full angle beam divergence (Ω'_{coll}) over the angular diameter of the Sun (Ω'_{Sun}). The collimator has a full angle beam divergence of 0.031° at 1370 nm. The Sun has an angular diameter of 0.531° which was calculated from the Sun's diameter (1.39×10^6 km) and the distance from Earth to the Sun (150×10^6 km). Hence, the ratio of the solid angles is $\Omega'_{coll}/\Omega'_{Sun} = 2\pi(1 - \cos 0.0155°)/2\pi(1 - \cos 0.266°) = 1/295$. In this approximation, the collimator effectively receives photons from 1/295 of the Sun's area. The effective collection area of the collimator (A'_{coll}) is calculated using the focal length of the collimator lens and the half angle of acceptance for the single mode fibre θ_{SM}. The focal length of the collimator lens is 18.67 mm. The SMF has $\theta_{SM} = 78.57 \times 10^{-3}$ rad $= 4.5°$ at 1370 nm. Hence, the effective diameter of the collimator within θ_{SM} is 2.94 mm and the effective collection area is $A'_{coll} = \frac{\pi}{4}(2.94 \times 10^{-3})^2 = 6.79 \times 10^{-6}$ m^2.

The estimated photons.s^{-1}.m^{-2} around 1370 nm within a 10 nm passband filter can be approximated using Figure 28b. It can be seen in this figure that the orders of magnitude range from 10^{11} and 10^{12} on average between 1365 – 1375 nm. In order to estimate the number of photon counts per second (CPS) from sunlight, it is assumed the 10 nm passband filter has a transmittance of 0.67 across all wavelengths. Similarly, the SPAD module is assumed to have a detection efficiency of 10% across all wavelengths. Hence, for the lower estimate of $10^{11}\ \text{photons.}\,\text{s}^{-1}.\,\text{m}^{-2}.\,\text{nm}^{-1}$, the estimated number of photon counts per second is $(10^{11}\ \text{photons.}\,\text{s}^{-1}.\,\text{m}^{-2}.\,\text{nm}^{-1})(10\ \text{nm})(0.67)(\frac{1}{295})(6.79 \times 10^{-6}\ \text{m}^2)(0.1) = 1{,}542$ CPS. Therefore, the estimated photon counts per second from sunlight ranges between 1,542 – 15,420 CPS.

3.2.3 Estimated and Measured Results

Table 11 shows the estimated and measured photon counts per second. The top three rows of Table 11 show the estimated total photon counts the SPAD module would receive using method 1 with the measured spectra from the NIR Flame spectrometer. The fourth row shows the estimated range of photon counts using method 2. The bottom two rows show the measured photon counts per second from the SPAD module. The maximum measurements of the SPAD module were obtained by directing the experimental apparatus towards the source to ensure the maximum number of photons were entering into the SPAD module. The minimum measurements of the SPAD module were obtained by directing the apparatus away from the source, e.g. in the case of direct sunlight, the apparatus was pointed away from the sun and up towards the clear sky. The measurements were averaged over two minutes and over this time the average was stable.

Table 11: Estimated and measured photon counts per second for the different ambient light scenarios.

Type of measurement	Range of measurement	Outside Sunny 100k lx	Outside Cloudy 30k lx	Inside 12k lx	LED lighting 100k lx
Method 1: Spectrum (estimated)	1015 – 1654 nm	6,426	1,994	389	1,160
Method 1: Spectrum (estimated)	1351 – 1414 nm	5,242	1,759	373	1,115
Method 1: Spectrum (estimated)	1367 – 1377 nm	3,828	1,437	241	861
Method 2: Angular FOV (estimated)	1365 – 1375 nm	1,542 – 15,420	n/a	n/a	n/a
SPAD module (measured)	Maximum	7,000	1,800	500	900
SPAD module (measured)	Minimum	2,000	1,300	500	500

Across the four experiments, there is variation between the measured and estimated data for ambient light at 100k lx, 30k lx, and 12k lx.

1) **Outside Sunny 100k lx**

The ‘Sunny: 100k lx’ measured spectrum tracks well with the ASTM reference standard. The estimated photon counts for the ‘Sunny: 100k lx’ spectrum from 1015 – 1654 nm using method 1 are in good agreement with the maximum measured photon counts from the SPAD. The estimated counts for the ‘Sunny: 100k lx’ spectrum are 6,426 CPS which are comparable to the measured maximum 7,000 CPS. There are a significant number of photon counts outside of the passband of the filter (1367 – 1377 nm). The measured 7,000 CPS are much greater than the estimated 3,828 CPS within the 10 nm passband. The estimated and measured photon counts per second are within the estimated range (1,542 – 15,420 CPS) using method 2.

2) **Outside Cloudy 30k lx**

The ‘Cloudy: 30k lx’ spectrum is as expected in terms of scale compared to the ‘Sunny 100k lx’ spectrum. The estimated photon counts for the ‘Cloudy: 30k lx’ spectrum from 1015 – 1654 nm using method 1 are in good agreement with the maximum measured photon counts from the SPAD. The estimated counts for the ‘Cloudy: 30k lx’ spectrum are 1,994 CPS which are comparable to the measured maximum 1,800 CPS. There are some photon counts outside of the passband of the filter (1367 – 1377 nm). The measured 1,800 CPS are greater than the estimated 1,437 CPS within the 10 nm passband.

3) **Inside 12k lx**

The ‘Inside: 12k lx’ spectrum is different from the outdoor solar spectra due to the coating on the double-glazed windows. The estimated photon counts for the ‘Inside: 12k lx’ spectrum using method 1 are 389 CPS which are below the 500 dark counts of the SPAD module. The measurements show there is no ambient light induced noise at the SPAD module. The dark counts are the dominant noise factor.

4) **LED lighting 100k lx**

The estimated photon counts based on the ‘LED: 100k lx’ spectrum using method 1 are in good agreement with the measurements by the SPAD module. The estimated counts for the ‘LED: 100k lx’ spectrum ranges from 861 CPS within the 10 nm passband to 1,160 CPS. Both estimates are comparable to the measured maximum 900 CPS.

3.3 QBER Estimation in Sunlight at 1370 nm

The measurements made by the SPAD module were used in the QKD link model from chapter 2 in order to investigate 1370 nm as a potential QKD wavelength of operation. Figure 31 shows the BB84 receiver design used in the QKD link model. In the receiver design, a spectral filter (Spectrogon 10 nm passband filter) centred at 1370 nm is used to mitigate the ambient light entering the receiver. 25% of the incident photons reach each detector.

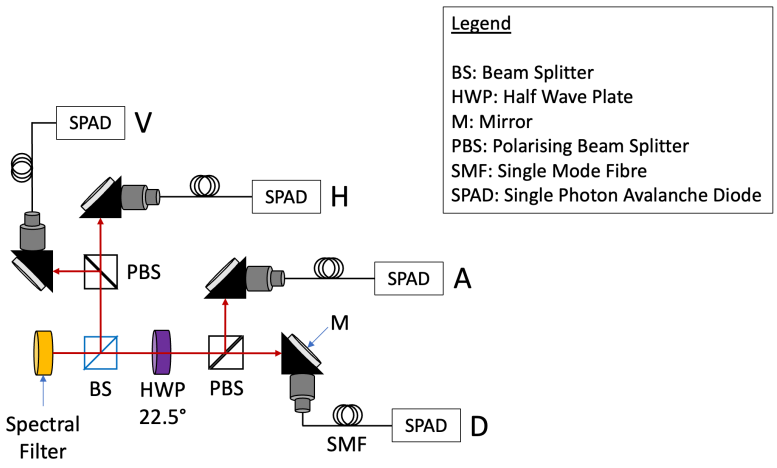


Figure 31: BB84 receiver design [114]. The received photons from sunlight are filtered by the spectral filter and are split into two paths: Horizontal/Vertical (H/V) and Diagonal/Anti-diagonal (D/A). The mirrors are used to align the received photons with the collimators at the front end of the single mode fibres and minimise the coupling losses into the SPAD modules. The SPAD modules receive 25% of the incident photons on the receiver.

The QBER of a QKD link was estimated based on the BB84 receiver design in Figure 31 and measured photon counts per second in Table 11. The Eq. (6) from chapter 2 section 2.1.1 was used to estimate the QBER with the QKD link parameters of H. Chun et al. in chapter 2 Table 2. However, a detector efficiency of $\eta = 0.1$ was used instead. R_{noise} is the total noise count rate per SPAD (CPS) that includes the dark counts and the sunlight. Figure 32 shows plots of the results of the QKD link simulations based on R_{noise} for the worst-case scenario in direct sunlight and the effect of varying link losses L_L. The link loss of 14 dB is the maximum threshold used in the QKD link simulations. The QKD link simulations assumed a fixed power

level at the transmitter, determined by the mean photon number and pulse rate. A fixed value for the mean photon number (μ) was used.

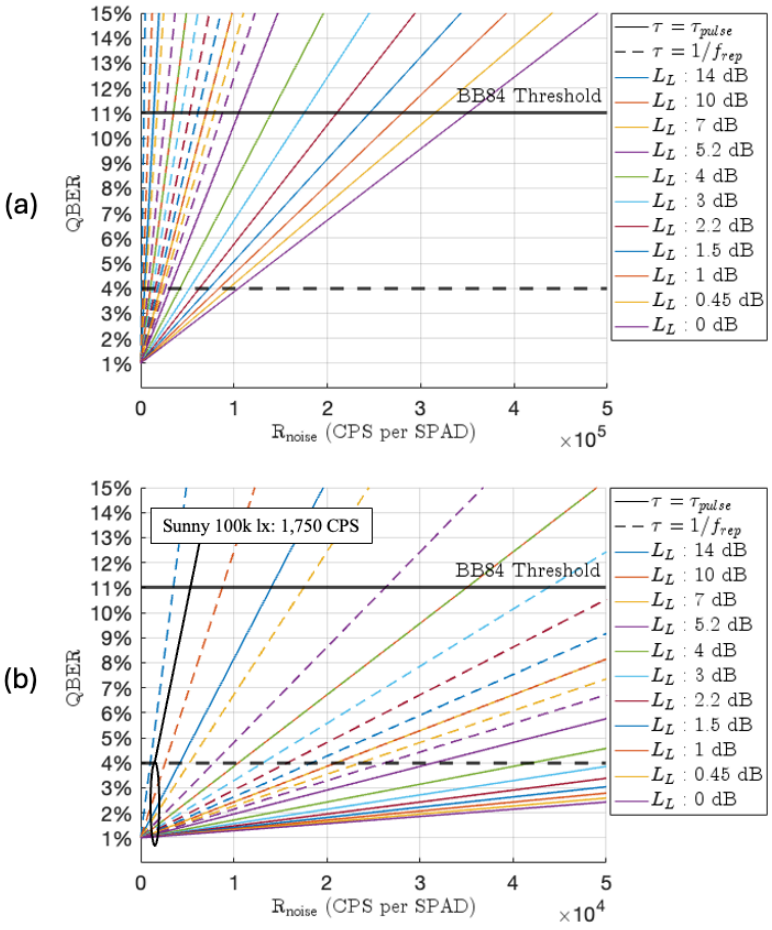


Figure 32: Plot of QBER vs total noise count rate per SPAD for QKD link simulations under filtered sunlight at 1370 nm. The QKD links were simulated for two scenarios: 1) temporal filtering with a gating window ($\tau = \tau_{pulse} = 1$ ns) and 2) no temporal filtering ($\tau = \frac{1}{f_{rep}} = 4$ ns). No temporal filtering was used to show the minimum link tolerance for noise. The QKD links were simulated at various link losses (L_L). The maximum link loss is 14 dB which corresponds to μ = 0.1 for a realistic beam splitter attack. (a) The link simulations where the QBER exceeds the BB84 threshold. (b) A subset of the link simulations where the QBER exceeds the practical threshold of 4%. The link losses were grouped together based on the estimated noise count rate for the worst-case scenario in direct sunlight (row 4 in Table 11).

It can be seen in Figure 32 that a BB84 link with a 10 nm passband filter centred at 1370 nm should tolerate direct sunlight and operate well below the 11% threshold depending on the link

loss and gating window. A QKD receiver was simulated under direct sunlight by using the total noise count rate per SPAD, $R_{noise} = 1{,}750$ CPS. It can be seen in Figure 32b that a QKD link with a gating window ($\tau = \tau_{pulse} = 1$ ns) can operate in direct sunlight with a QBER below 4% and potentially tolerate a 14 dB link loss. A QKD link without temporal filtering ($\tau = \frac{1}{f_{rep}} =$ 4 ns) can operate in direct sunlight with a QBER below 4% and potentially tolerate a 10 dB link loss. For higher ambient light levels and noise counts (exceeding 100k lx sunlight), a QKD link performance with lower link losses can be tolerated [265]. The link simulation suggests a QKD receiver without temporal filtering could tolerate 3 times the lux level (300k lx) of direct sunlight and maintain a QKD link with 7 dB link loss. Furthermore, at 300k lx a QKD receiver could use a gating window ($\tau = \tau_{pulse} = 1$ ns) and maintain a QKD link with 14 dB link loss at QBER = 4.5%. Also, in the most extreme scenario a QKD receiver without temporal filtering could tolerate the maximum noise count rate per SPAD ($R_{noise} = 7{,}000$ CPS) and still maintain a link with 5.2 dB link loss at QBER = 4%. Similarly, for $R_{noise} = 7{,}000$ CPS, a QKD receiver could use a gating window ($\tau = \tau_{pulse} = 1$ ns) and maintain a link with 10 dB link loss at QBER = 3%.

3.4 Discussions and Observations

Table 12: Results summary of QKD link simulations at 1370 nm.

Results Summary of the QKD Link Simulations at 1370 nm	
Filter bandwidth (nm)	10
Sunlight – 100k lx R_{noise} using η = 0.1 (CPS per SPAD)	1,750
	Maximum link loss tolerance (dB)
$\tau = \tau_{pulse} = 1$ ns	14
$\tau = \frac{1}{f_{rep}} = 4$ ns	14
	Link loss tolerance at QBER = 4% (dB)
$\tau = \tau_{pulse} = 1$ ns	14
$\tau = \frac{1}{f_{rep}} = 4$ ns	10
QKD link works under sunlight? ($L_L = 7$ dB threshold)	Yes

Table 12 shows a summary of the results for the QKD link simulations for a wavelength of operation at 1370 nm. The decreased photon counts due to sunlight enabled a QKD receiver to work with wider passband filters such as the 10 nm Spectrogon interference filter centred at 1370 nm.

3.5 Summary

In this chapter, a wavelength region in which to operate a QKD link that is robust to ambient light was proposed. We identified the 1351 – 1414 nm band as a promising wavelength region, and more specifically the wavelengths around 1370 nm, in which to operate an indoor free-space QKD link. We designed an experimental apparatus to measure the photon counts, spectrum, and lux levels for four sets of experiments: 1) outside under clear skies in direct sunlight at 100k lx, 2) outside under cloudy skies at 30k lx, 3) inside a meeting room with windows and ambient light only, and 4) in a laboratory under LED ceiling lighting only. The experimental measurements showed that a BB84 link should operate at 1370 nm because the ambient light in this region had minimal effect on a BB84 QKD receiver. The influence of

ambient light on the QKD link performance at 1370 nm was simulated and showed a link could work in sunlight with a 10 nm bandwidth filter. The QKD link worked for link losses of 10 – 14 dB depending on whether no temporal filtering ($\tau = \frac{1}{f_{rep}} = 4$ ns) or a gating window was used ($\tau = \tau_{pulse} = 1$ ns). The QKD link performance was capable of a higher tolerance for noise much greater than 100k lx sunlight at 1370 nm. In the most extreme scenario, the QKD receiver could tolerate a maximum noise count rate $R_{noise} = 7{,}000$ CPS and still maintain a link loss of 5.2 dB without temporal filtering ($\tau = \frac{1}{f_{rep}} = 4$ ns) at QBER = 4%. Similarly, a QKD link could still maintain a link loss of 10 dB with a gating window ($\tau = \tau_{pulse} = 1$ ns) at QBER = 3%. The next chapter details an experiment that tests a QKD system, designed for 1371.5 nm and the BB84 protocol, with the receiver under a halogen lamp as a suitable substitute for ambient sunlight in the 1351 – 1414 nm region.

Chapter 4 BB84 Free-space Experiment at 1371.5 nm under Ambient Light

In this chapter, we report the results of a proof of concept BB84 free-space QKD link designed at a novel wavelength of operation and implemented under different lighting conditions. The purpose of the experiments is to show how ambient light affects the QBER of a free-space QKD link around 1370 nm. The results of these experiments can help estimate the effect of ambient light on an actual QKD link. The operational wavelength of the QKD link was 1371.5 nm and the QKD link was a benchtop demonstration in a laboratory. The chapter begins with the calibration of a halogen lamp as an analogue for sunlight around 1370 nm and QKD link simulations under the illumination from the halogen lamp. Then the rest of the chapter focuses on the experimental apparatus, the characterisation of the transmitter and receiver, experimental methodology, and performance results of the QKD link.

4.1 Halogen Lamp Calibration

In the previous chapter (Chapter 3 section 3.2), a set of experiments were conducted to measure the spectrum and lux levels of four scenarios: 1) outside in direct sunlight at 100k lx, 2) outside under cloudy skies at 30k lx, 3) inside a meeting room with sunlight passing through double-glazed windows at 12k lx, and 4) inside a laboratory with LED ceiling lighting (100k lx at the sources). It was shown in Chapter 3 Figure 30b that the measured outdoor spectrum 'Sunny: 100k lx' was relatively flat between 1351 – 1414 nm. In order to simulate the same level of sunlight as 'Sunny: 100k lx' in the 1351 – 1414 nm region, a halogen lamp (RS Components 569 – 947) was used because the spectral response was flat across the 1351 – 1414 nm bandwidth.

An experiment was conducted to calibrate the halogen lamp to simulate a solar source between the 1351 – 1414 nm region in a laboratory. The halogen lamp was placed in front of and pointed directly at the experimental apparatus. The experimental apparatus consisted of a calibrated NIR Flame spectrometer (6 nm resolution) with Ø600 µm fibre and cosine corrector (Ocean Insight FLAME-NIR-INTSMA25) used to measure the spectrum and an Amprobe LM-100 lux meter used to measure the lux level. The cosine corrector had 2π steradian field of view. The spectrometer was connected to a laptop via USB in order to view the measured spectrum in real-time. The halogen lamp was moved away from the spectrometer until the measured spectrum was comparable to the 'Sunny: 100k lx' level between 1351 – 1414 nm. This resulted in the halogen lamp placed at a distance of 60 cm away from the apparatus and 800 lx measured by the Amprobe LM-100 lux meter.

Figure 33 shows plots of the measured halogen spectrum at 800 lx with the previously measured spectra from Chapter 3 section 3.2 in $\log_{10}(\text{photons.s}^{-1}.\text{m}^{-2}.\text{nm}^{-1})$ vs wavelength. The measured spectra from section 3.2 are plotted to compare with the simulated sunlight source (halogen lamp). The ASTM AM1.5 spectrum is used as reference. Figure 33a shows a plot of the measured spectra in $\log_{10}(\text{photons.s}^{-1}.\text{m}^{-2}.\text{nm}^{-1})$ vs wavelength. Figure 33b shows a plot of the measured spectra from 1351 – 1414 nm in $\log_{10}(\text{photons.s}^{-1}.\text{m}^{-2}.\ \text{nm}^{-1})$ vs wavelength.

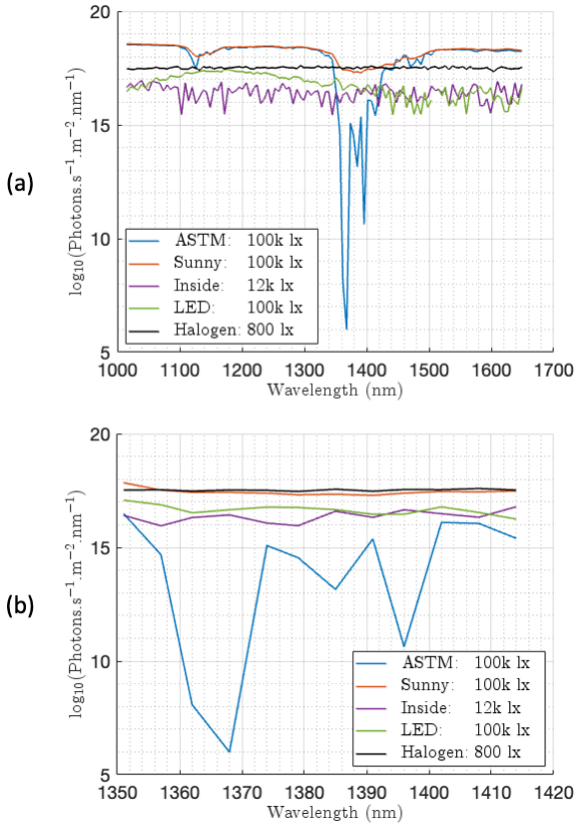


Figure 33: Plots of the measured ambient light spectra with measured halogen spectrum at 800 lx. (a) Plot of measured spectra by the NIR Flame spectrometer in $\log_{10}(\text{photons.s}^{-1}.\text{m}^{-2}.\text{nm}^{-1})$ vs wavelength and (b) plot of measured spectra from 1351 – 1414 nm region in $\log_{10}(\text{photons.s}^{-1}.\text{m}^{-2}.\text{nm}^{-1})$ vs wavelength. The measured spectra from Chapter 3 section 3.2 are shown in the plots to compare with the simulated sunlight ('Halogen: 800 lx') measured spectrum. The ASTM AM1.5 spectrum is used as reference.

It can be seen in Figure 33 that the 'Halogen: 800 lx' spectrum is flat across the entire bandwidth of the spectrometer. More specifically, the 'Sunny: 100k lx', 'Halogen: 800 lx', and 'ASTM: 100k lx' spectra in Figure 33b were analysed. The 'Sunny: 100k lx' and 'Halogen: 800 lx' spectra were integrated across the 1351 – 1414 nm region. The integrations showed that these two spectra were approximately equal. The 'ASTM: 100k lx' spectrum was integrated across the same region for comparison. The integral of 'Halogen: 800 lx' spectrum was 8x the integral of the 'ASTM: 100k lx' spectrum. That is, the halogen lamp was equivalent to 800,000 lx outdoor sunlight in the 1351 – 1414 nm region. The halogen lamp was comparable to the

outdoor measured spectrum and a suitable substitute for sunlight in the region of 1351 – 1414 nm.

In the final experiment, the BB84 QKD receiver was placed inside a blackout box with an aperture at the front of the receiver. In order to test the BB84 QKD system at 1371.5 nm under sunlight, the halogen lamp was placed 60 cm away from the front of the QKD receiver. The halogen lamp was pointed directly at the front of the QKD receiver. Figure 34 shows a picture of the halogen lamp illuminating the QKD receiver inside the blackout box in the experimental setup.

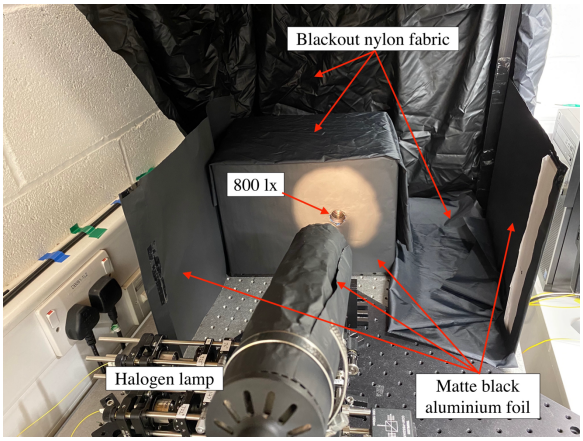


Figure 34: Picture of the halogen lamp illuminating the QKD receiver inside the blackout box. The halogen lamp was located 60 cm away from the QKD receiver. 800 lx was measured in front of the aperture of the QKD receiver.

Black aluminium foil was secured around the halogen lamp to confine the beam directly onto the QKD receiver aperture. The Amprobe LM-100 lux meter was used at the input to the QKD receiver and measured 800 lx. The QKD receiver used two types of SPAD modules: ID Quantique id221 with single mode fibre input and idQube low-noise model with single mode fibre input. These SPAD modules were used to count the photons from the halogen lamp in each H, V, D, A path. Each SPAD module was in free-running mode with a PDE of 10% and a

dead time of 25 µs. The maximum photon counts from the halogen lamp for either SPAD module was 800 CPS.

4.2 QKD Link Simulations under Halogen Lamp

In the final experiment, a ID900 Time Controller was used to control the output pulses of the QKD transmitter. The maximum repetition rate for the ID900 was 41.67 MHz which was set by running the system at a period of 24 ns. The final experiment ran for two repetition rates: 41.67 MHz and 10 MHz. Two repetition rates were used to show the experiment was repeatable and the results were reproducible. The QKD link was simulated under the illumination of the halogen lamp for repetition rates 41.67 MHz and 10 MHz in order to compare with the final experimental performance results. Similar to section 3.3, the QBER of a QKD link was estimated based on the BB84 receiver design in Figure 31 and measured photon counts per second from the halogen lamp at 800 lx. The Eq. (6) from chapter 2 section 2.1.1 was used to estimate the QBER with the QKD link parameters in Table 13. R_{noise} is the total noise count rate per SPAD (CPS) that includes the dark counts and illumination from the halogen lamp.

Table 13: QKD link simulation parameters for repetition rates 41.67 MHz and 10 MHz.

QKD Link Simulation Parameters	
Mean photon number (μ)	0.1
Repetition rate (f_{rep})	41.67 MHz and 10 MHz
Detector efficiency (η)	0.1
Polarisation error (p_{opt})	0.01
Number of detectors (n)	4

Figure 35 shows plots of the results of the QKD link simulations for repetition rate 41.67 MHz based on R_{noise} under the halogen lamp at 800 lx and the effect of varying link losses.

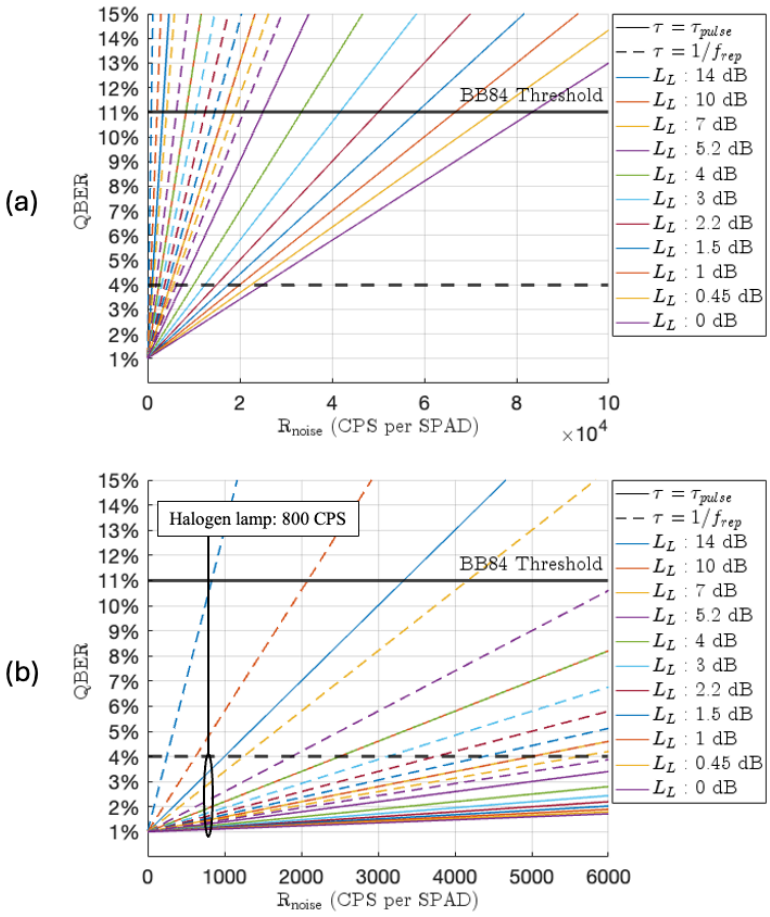


Figure 35: Plot of QBER vs total noise count rate per SPAD for QKD link simulations at 41.67 MHz under the halogen lamp at 800 lx.The QKD links were simulated for two scenarios: 1) temporal filtering with a gating window ($\tau = \tau_{pulse} = 6$ ns) and 2) no temporal filtering ($\tau = \frac{1}{f_{rep}} = 24$ ns). No temporal filtering was used to show the minimum link tolerance for noise. The QKD links were simulated at various link losses (L_L). The maximum link loss is 14 dB which corresponds to μ = 0.1 for a realistic beam splitter attack. (a) The link simulations where the QBER exceeds the BB84 threshold. (b) A subset of the link simulations where the QBER exceeds the practical threshold of 4%. The link losses were grouped together based on the measured noise count rate for the halogen lamp at 800 lx.

Similarly, Figure 36 shows plots of the results of the QKD link simulations for repetition rate 10 MHz. The link loss of 14 dB is the maximum threshold used in the QKD link simulations.

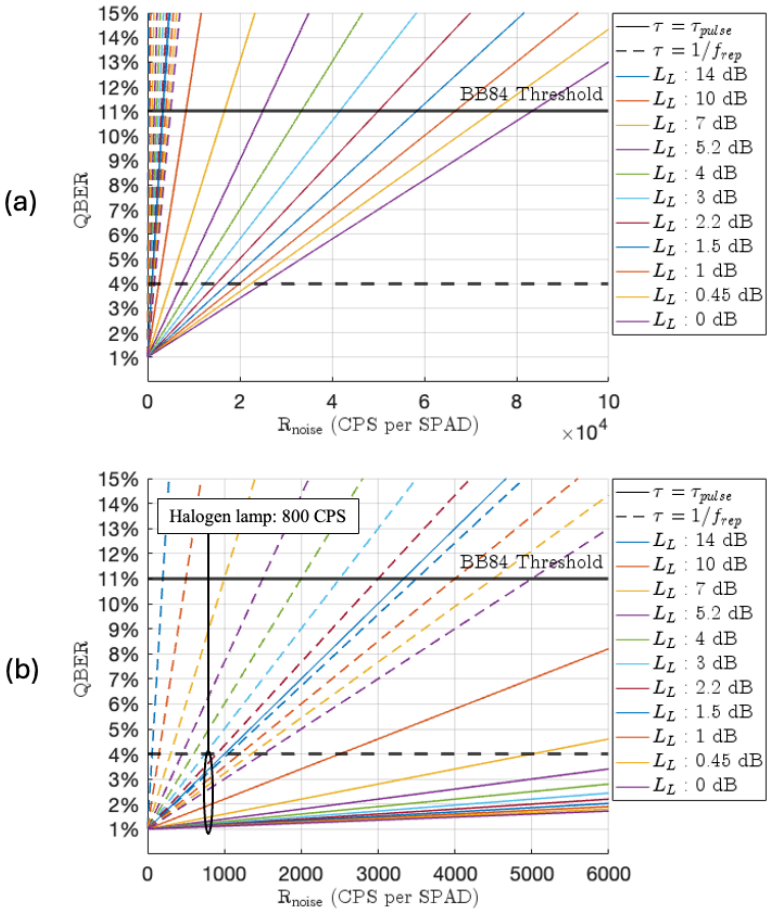


Figure 36: Plot of QBER vs total noise count rate per SPAD for QKD link simulations at 10 MHz under the halogen lamp at 800 lx.Similar to Figure 35, the QKD links were simulated for two scenarios: 1) temporal filtering with a gating window ($\tau = \tau_{pulse} = 6$ ns) and 2) no temporal filtering ($\tau = \frac{1}{f_{rep}} =$ 100 ns). (a) The link simulations where the QBER exceeds the BB84 threshold. (b) A subset of the link simulations where the QBER exceeds the practical threshold of 4%. The link losses were grouped together based on the measured noise count rate for the halogen lamp at 800 lx.

The results of the QKD link simulations show that a QKD system operating at 1371.5 nm for both repetition rates is feasible and robust to sunlight, especially with a gating window ($\tau = \tau_{pulse} = 6$ ns). It can be seen in Figure 35b and Figure 36b that a QKD link with a gating window ($\tau = \tau_{pulse} = 6$ ns) can operate under the halogen lamp with a QBER below 4% and

potentially tolerate a 14 dB link loss. Figure 35b also shows that the QKD link should work without temporal filtering ($\tau = \frac{1}{f_{rep}} = 24$ ns) with QBER = 4% up to 7 dB link loss and at the maximum QBER threshold up to 14 dB link loss. Similarly, Figure 36b shows that the QKD link should work without temporal filtering ($\tau = \frac{1}{f_{rep}} = 100$ ns) with QBER = 4% up to 2.2 dB link loss and at the maximum QBER threshold up to 7 dB link loss. The next sections detail the experimental apparatus, the characterisation of the transmitter and receiver, the experimental methodology, and performance results of the BB84 free-space link.

4.3 Experimental Apparatus

This section describes how the QKD transmitter and receiver in the experimental apparatus were configured and implemented for the BB84 protocol. Each component of the QKD transmitter and receiver are described in detail.

4.3.1 Transmitter

Figure 37 shows a picture of the QKD transmitter apparatus. The QKD transmitter apparatus consisted of the laser driver assembly and the QKD transmitter assembly.

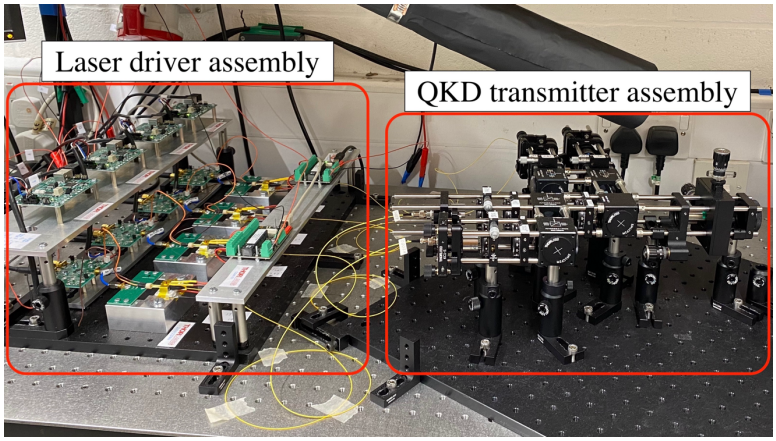


Figure 37: Picture of the experimental QKD transmitter apparatus that consisted of the laser driver assembly and the QKD transmitter assembly.

Figure 38 shows the block diagram of the QKD transmitter assembly for the BB84 protocol. The transmitter (Alice) consisted of four single mode fibre lasers (Roithner Lasertechnik SPL1370-2-9-PD) that were collimated (Thorlabs F810FC-1310). Each laser had an optical path consisting of a linear polariser (Thorlabs LPIREA100-C), half wave plate (Thorlabs WPH10E-1310), and polarising beam splitter (Thorlabs CCM1-PBS254/M) to ensure a 'p' or 's' polarisation. The additional half wave plate (WPH10E-1310) at 22.5° half angle (45° full angle) was used to rotate the 'p' and 's' polarisation to create the Diagonal and Anti-diagonal bases. All bases were combined into a 50:50 non-polarising beam splitter (Edmund Optics #47-236). The spatial filter was made up of two lenses (Thorlabs C240TMD-C, LA1540-C-ML) and a Ø5 µm pinhole (Thorlabs P5K). The output beam power was further attenuated with an iris (Thorlabs SM1D12C) that had a maximum aperture of Ø12 mm.

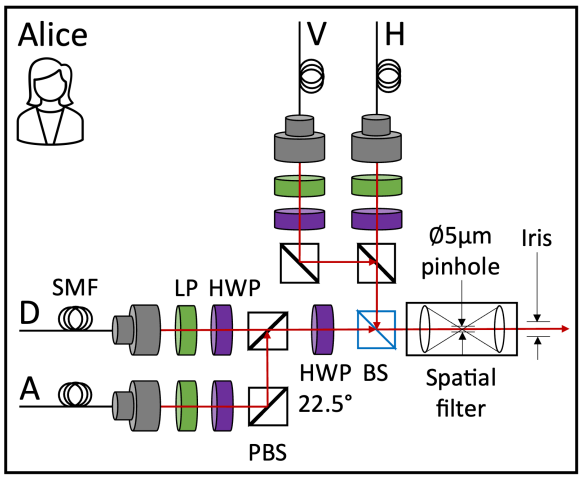


Figure 38: Block diagram of the QKD transmitter assembly. The terms used are **SMF**: Single Mode Fibre, **LP**: Linear Polariser, **HWP**: Half Wave Plate, **PBS**: Polarising Beam Splitter, **BS**: Beam Splitter, **H**: Horizontal, **V**: Vertical, **D**: Diagonal, **A**: Anti-diagonal.

4.3.1.1 Laser Sources

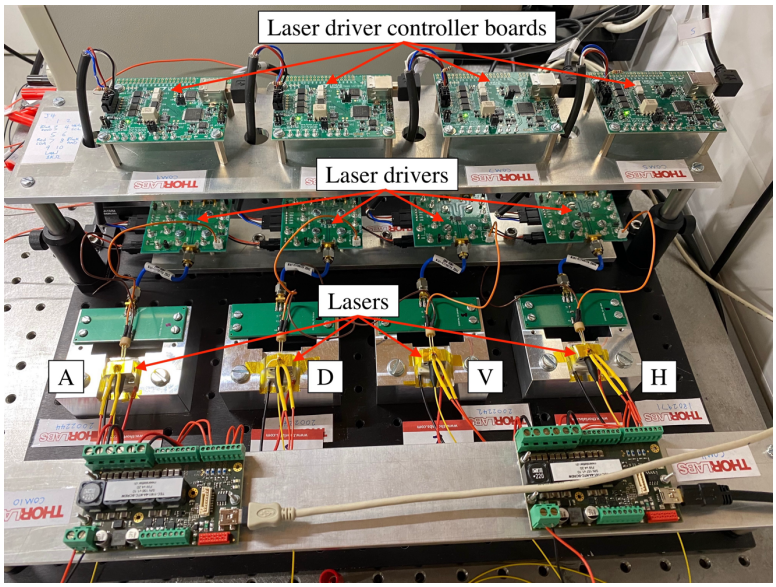


Figure 39: Picture of lasers, laser drivers, and controller boards in the laser driver assembly. The transmitter lasers are **H**: Horizontal, **V**: Vertical, **D**: Diagonal, **A**: Anti-diagonal.

Figure 39 shows a picture of the lasers, laser drivers, and controller boards in the laser driver assembly. The four transmitter sources were single mode fibre lasers from Roithner Lasertechnik (SPL1370-2-9-PD). The SPL1370-2-9-PD was a distributed feedback (DFB) laser that had a centre wavelength of 1370 nm (±2 nm) and spectral bandwidth of 0.3 nm. This DFB laser operated in Continuous Wave (CW) mode with 2 mW average power and could operate at up to 1.25 gigabit/s data rate. Each laser was DC biased by a laser driver (Analog Devices DC499A [266]) with an AC input for modulation from an external source. This driver was a Vertical Cavity Surface Emitting Laser (VCSEL) driver capable of a 155 megabit/s to 3.2 gigabit/s data rate. It was operated in Constant Current Mode to ensure no thermal runaway in the event of improper cooling. The settings were configured by the laser driver controller boards (Analog Devices DC590B [267]).

The four lasers were modulated by a ID900 Time Controller. The ID900 Time Controller was an instrument that was both a pattern generator and a time-correlated single-photon counter

(TCSPC). The ID900 used Field Programmable Gate Arrays (FPGAs) to generate pulses with short pulse widths and to receive pulses for photon counting. The received pulses were timestamped using the ID900 internal reference clock system and the ID900 displayed the photon counting in histograms of Photon counts vs Time bins. The ID900 had four output channels that send electronic pulses using the Nuclear Instrumentation Module (NIM) standard [268]. These pulses had an amplitude 0 V (logical false) and –0.8 V (logical true). The NIM pulses used at the QKD transmitter had 6 ns pulse width and these pulses were AC coupled into the laser driver. The laser driver had offset the pulse amplitude by 50% which resulted in a pulse amplitude at ±0.4 V. Each laser transmitted a NIM pulse with +0.4V amplitude and 6 ns FWHM pulse width.

4.3.1.2 Temperature Controller

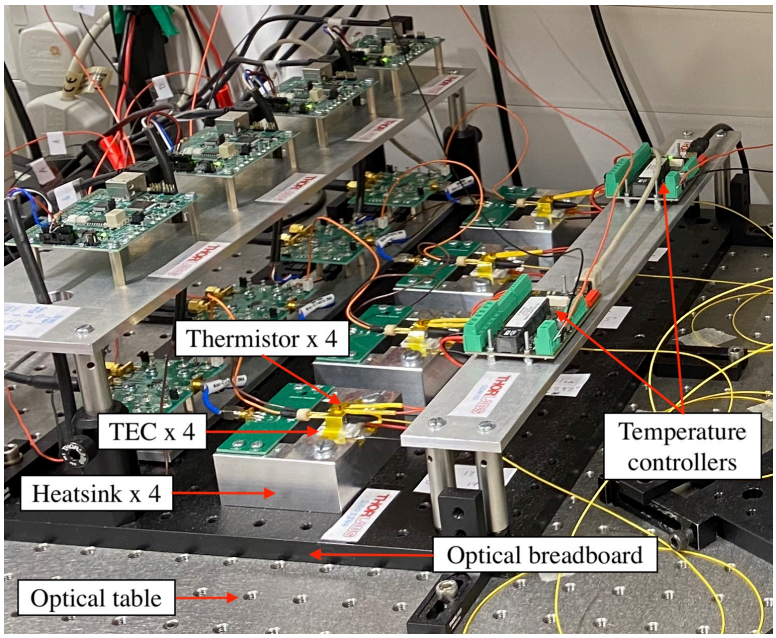


Figure 40: Picture of temperature controllers, thermistors, TEC elements, and heatsink components in the laser driver assembly.

Figure 40 shows a picture of the temperature controllers, thermistors, TEC elements, and heatsink components in the laser driver assembly. The four lasers must be temperature

controlled to operate efficiently at the desired wavelength as the centre wavelengths of the lasers shift based on the operating temperature. The lasers were temperature controlled with two Meerstetter Engineering controller boards (TEC-1161-4A-NTC-SCREW [269]) and four Peltier elements (Thorlabs TECF1S) to align the centre wavelengths of all four lasers. Each Meerstetter Engineering controller board could operate two channels (±4 A, ±21 V) for a total cooling capacity of 84 W (up to 42 W per channel). One 10 kΩ NTC thermistor (Vishay NTCLE100E3103JT2) was mounted on top of each laser for temperature feedback into the temperature controller boards to maintain a constant temperature. The lasers were mounted on top of the cold side of the Peltier elements while the hot side of the Peltier element was mounted on top of an aluminium heatsink, optical breadboard, and the optical table. The stacked combination of the heatsink, optical breadboard, and optical table acted as an effectively large heatsink. The Thorlabs TECF1S peltier elements were suitable components to align the centre wavelengths because the initial centre wavelengths across all of the lasers were close. Table 14 shows the four lasers and their wavelength characteristics based on temperature.

Table 14: Centre Wavelength Parameters for Lasers.

Laser Serial Number	**Polarisation Basis**	**Initial centre wavelength (nm) in the laboratory (~22 – 23˚C)**	**$\frac{\Delta\ \text{nm}}{^{\circ}\text{C}}$**	**Centre Wavelength (nm)**	**Final temperature setting (˚C)**
1802971	H	1371.700	0.1536	1371.503	20.04
2002242	V	1370.706	0.1285	1371.503	28.15
2002243	D	1370.497	0.1179	1371.503	32.37
2002244	A	1371.325	0.1210	1371.503	23.59

The lasers (SPL1370-2-9-PD) had an operating temperature range of -10 to +85 ˚C. The spectra were measured using an Agilent 86142B optical spectrum analyser with 0.002 nm resolution [270]. It can be seen in Table 14 that the largest delta between laser ‘H’ and laser ‘D’ is 1.203 nm. The delta equates to approximately 10 degrees Celsius which is a small temperature differential. Therefore, the alignment of the centre wavelengths can be done with a cost-

effective Peltier element. The laser for polarisation H was cooled and the other three lasers for polarisations V, D, and A were heated to operate at the final centre wavelength of 1371.503 nm.

4.3.1.3 Spatial Filter

Figure 41 shows a picture of the spatial filter in the QKD transmitter assembly.

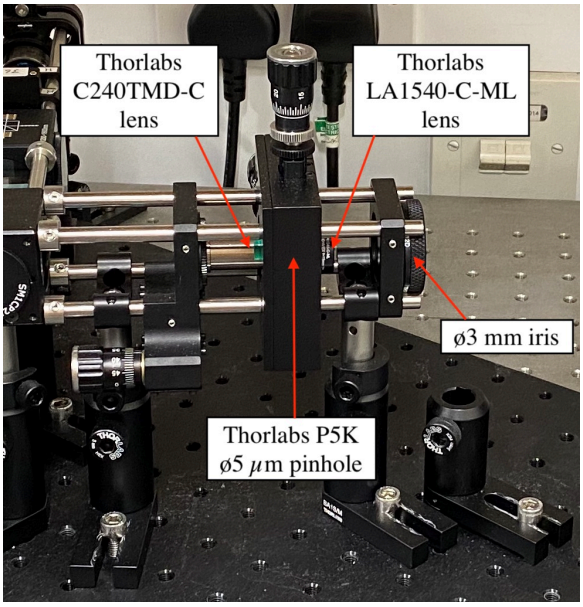


Figure 41: Picture of the spatial filter in the QKD transmitter assembly. The spatial filter was made up of two lenses and a pinhole. The output of the QKD transmitter assembly was an iris set to Ø3 mm.

In Figure 41 the four lasers were made spatially indistinguishable by passing the output laser beams through a common spatial filter. A spatial filter was an apparatus made up of two lenses and a pinhole that ensured all light beams were output with the same beam shape and had maximum overlap when transmitted. The four lasers were aligned in position and direction using a calibrated Newport 1830-C power meter at the output of the spatial filter. The power of each laser was measured at the output of the spatial filter and again at the front of the QKD receiver. This ensured the laser beams were overlapped and aligned prior to entering the QKD receiver. For each laser, the half wave plate that was located in between the linear polariser and polarising beam splitter was rotated to ensure the maximum power levels were the same.

However, it was assumed the four laser beams overlap at their maxima using only the maximum power levels measured over the transverse axes at the entrance of the QKD receiver. There was no equipment available in our laboratory to capture an image of the four laser beams overlapping.

In Figure 41 all light was focused from the first lens (Thorlabs C240TMD-C) into a Ø5 µm pinhole (Thorlabs P5K). This pinhole removed the high spatial frequency noise (outer diffraction rings) of the transmitted Gaussian beams and only allowed the central Gaussian spot (fundamental mode TEM_{00}) to pass through. The Gaussian spots from the four transmitters were then collimated by the second lens (Thorlabs LA1540-C-ML) and into a Ø3 mm iris at the output of the transmitter. The diameter of the pinhole was calculated using equation (25) [271]

$$D = \frac{\lambda f}{r} \tag{25}$$

where D is the diffraction-limited spot size of the central Gaussian spot, λ is the wavelength, f is the focal length, and r is the input beam radius at $\frac{1}{e^2}$ point. The diffraction-limited spot size must then be multiplied by 1.3 to get the ideal pinhole. If the pinhole was too small, the central Gaussian spot was partially blocked and if the pinhole was too large, more than the fundamental Gaussian mode was transmitted. The diameter of the pinhole was also a trade-off between ease of alignment and transmission loss. A larger pinhole offered easier alignment of the input laser beams, more power and less transmission loss through the spatial filter. However, this was at the expense of more Gaussian modes and high spatial frequency noise also transmitted through.

In the experiment, the input beam radius was half of the $\frac{1}{e^2}$ beam diameter output of the Thorlabs F810FC-1310 collimator and the beam divergence based on the path length of the laser collimator to the entrance of the spatial filter was considered. The full angle beam divergence at 1371.5 nm was approximately 0.025˚. The paths for each polarisation input (H, V, D, A) to

the spatial filter were similar lengths: H and D had a 235 mm path length and V and A had a 275 mm path length. The wavelength ($\lambda = 1371.5$ nm), the focal length of the C240TMD-C lens ($f = 8$ mm), and the maximum input beam radius ($r = 3.41$ mm) were substituted into equation (25) which yielded a diffraction-limited spot of 3.2 μm. Hence, a 4.2 μm ideal pinhole was recommended for the system. Consequently, the Thorlabs P5K Ø5 μm pinhole was chosen as the most suitable pinhole available from Thorlabs. The next smallest pinhole was Ø2 μm which is too small. The Ø5 μm pinhole was slightly larger than the ideal pinhole and, as a result, more power and more than just the central Gaussian spot was transmitted. Potentially more spatial modes of the Gaussian laser beams and high frequency noise were transmitted through.

The spatial filter was also an infinite/infinite conjugate system made of two lenses where the system takes incoming collimated light into the first lens and the outgoing light through the second lens is also collimated. The ratio of the beam widths was the same as the ratio of the focal lengths of the lenses. In this case, the spatial filter was a beam expander where the beam diameter of the outgoing collimated light was increased. The second lens of the spatial filter was chosen as LA1540-C-ML with a focal length of 15 mm to ensure the Gaussian beam profile was magnified for a minimum of Ø12 mm. The magnification of a lens is

$$M = \frac{q}{p} \tag{26}$$

where q is the distance from the image plane to the lens and p is the distance from the object plane to the lens. The magnification of the spatial filter system was therefore 1.875 and the output beam diameter was approximately Ø12.78 mm.

4.3.2 Receiver

Figure 42 shows a picture of the optical apparatus of the QKD receiver in the experimental setup.

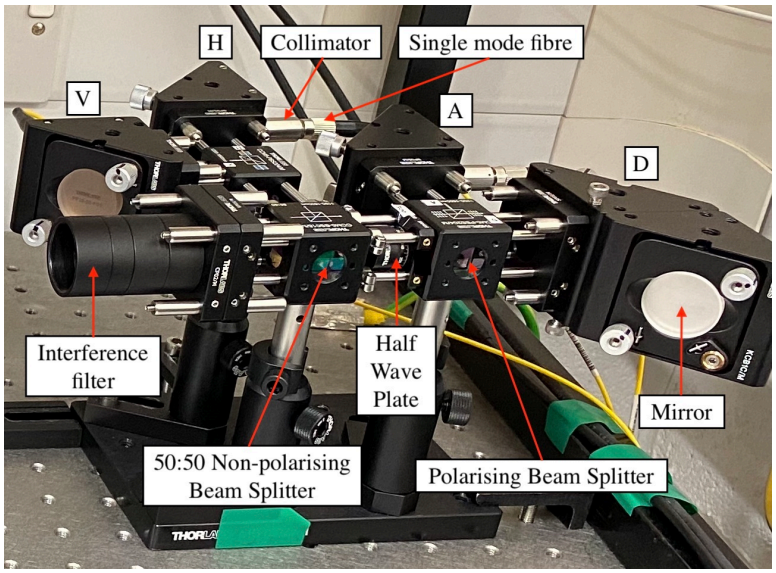
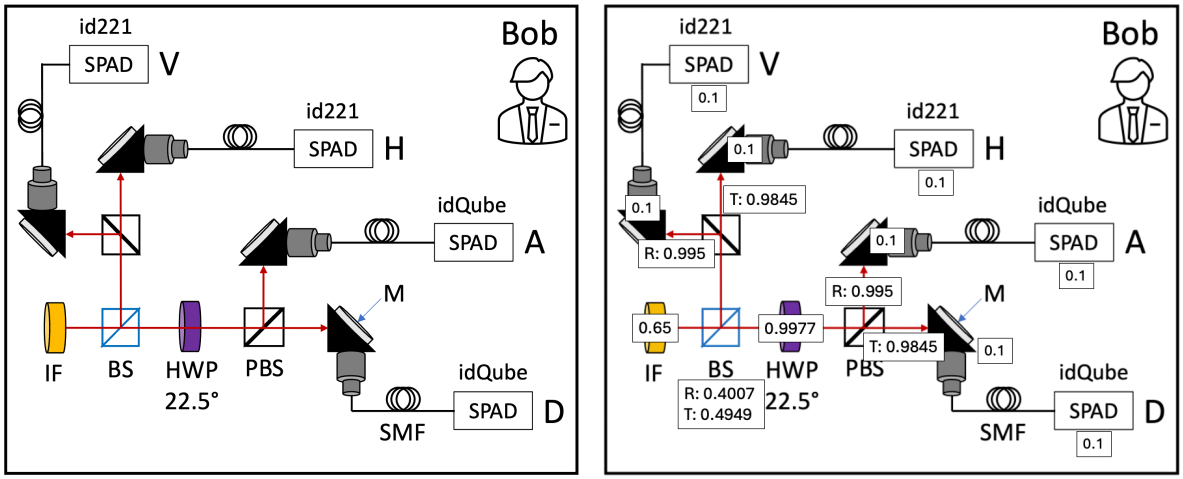


Figure 42: Picture of the optical apparatus of the QKD receiver in the experimental setup. The receiver ports are **H**: Horizontal, **V**: Vertical, **D**: Diagonal, **A**: Anti-diagonal.

Figure 43 shows the block diagram of the receiver for the BB84 protocol. Figure 43a shows the overall block diagram of the QKD receiver. Figure 43b shows the transmittance values of the components in the QKD receiver. The received photons were filtered by a 10 nm bandwidth interference filter (Spectrogon NB-1370-010). After the 50:50 non-polarising beam splitter (Thorlabs CCM5-BS018/M), the received photons were randomly sent down a path to either the H/V basis choice or the D/A basis choice. Each path had a polarising beam splitter (Thorlabs CCM5-PBS204/M) to differentiate between each basis choice. A half wave plate (Thorlabs WPHSM05-1310) was set to 22.5˚ to rotate the received photon polarisation for the D/A basis choice. The mirrors were used to align the incoming beam with the collimators (Thorlabs F280FC-C) to minimise the coupling losses into the SPAD modules. The collimators had a narrow field of view, and this limited side channel attacks from Eve. A potential type of side channel attack can occur when Eve and Alice are within the same field of view of Bob. If Alice

and Bob had already authenticated each other and established a quantum channel, Eve can pretend to be Alice and begin exchanging photons with Bob.



(a) (b)

Figure 43: Block diagrams of the QKD receiver. The terms used are **SMF**: Single Mode Fibre, **HWP**: Half Wave Plate, **PBS**: Polarising Beam Splitter, **BS**: Beam Splitter, **IF**: Interference Filter, **M**: Mirror, **H**: Horizontal, **V**: Vertical, **D**: Diagonal, **A**: Anti-diagonal, **SPAD**: Single Photon Avalanche Diode. (a) The overall block diagram of the QKD receiver. (b) The block diagram of the QKD receiver with transmittance values for each component. The 'T' and 'R' at the beam splitters denote Transmitted and Reflected paths respectively. The coupling between the silver mirror and the collimator was measured. The value at the SPAD is the PDE and was set to 0.1. The rest of the transmittance values were calculated from manufacturer specifications and datasheets.

Table 15 shows the component values used in the calculation of the overall transmittance for each receiver channel. The non-polarising beam splitter was not included in the calculation because it facilitated the bases choices. The transmittance values for the transmitted and reflected paths are manifested in the distribution of the received counts across all four channels. The average transmittance value across all four receiver channels is 0.0064.

Table 15: Transmittances of the four receiver channels.

Rx Channel	IF	PBS T	PBS R	HWP	Coupling	PDE	Transmittance
H	0.65	0.9845	-	-	0.1	0.1	0.0064
V	0.65	-	0.995	-	0.1	0.1	0.00646
D	0.65	0.9845	-	0.9977	0.1	0.1	0.00638
A	0.65	-	0.995	0.9977	0.1	0.1	0.00645

Figure 44 shows a picture of the QKD receiver inside a blackout box and the surrounding experimental apparatus with blackout nylon fabric and aluminium foil. The blackout box was covered with matte black aluminium foil and wrapped on all sides by blackout nylon fabric. Black aluminium foil was used as barriers around the receiver. This ensured the ambient light was only coming through the interference filter at the aperture of the receiver.

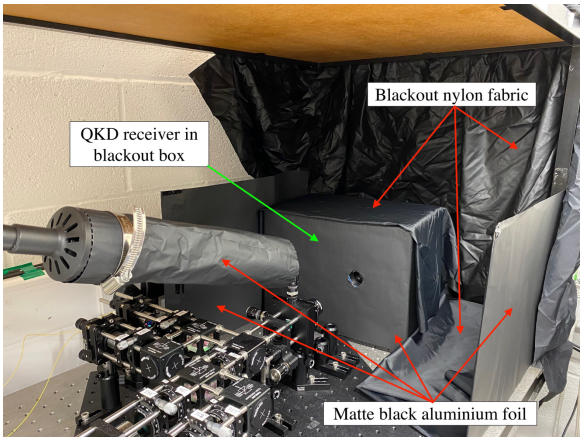


Figure 44: Picture of the QKD receiver inside blackout box and the surrounding experimental apparatus with blackout fabric and aluminium foil. This ensured the ambient light was only coming through the interference filter at the aperture of the receiver.

4.4 Experimental Characterisation of the Transmitter

This section describes the methodology of how the polarisation bases at the transmitter were calibrated and how the properties of each laser were made temporally, spectrally, and spatially indistinguishable to each other. The mean photon number of the transmitter is addressed.

4.4.1 Polarisation Angle Calibration

The polarisation of the transmitted photon is critical to basis detection at the receiver. The accuracy of the polarisation angle maximises the likelihood of the photons being detected by the correct SPAD. An experiment was conducted to measure the polarisation angle at the output of the spatial filter. The polarisation angle for each basis was measured with a linear polariser (Thorlabs LPIRE100-C) mounted in a continuous rotation mount (Thorlabs RSP1/M) with 360˚ scale markings in 2˚ increments. There were markings annotated on the mount that designated the linear polariser maximally aligned in the Horizontal position and maximally aligned in the Vertical position. This linear polariser inside the rotation mount was calibrated in a separate experiment prior to the assembly of the QKD transmitter. The calibration of the linear polariser used one of the lasers at the transmitter, linear polariser, half wave plate, polarising beam splitter, another linear polariser, and calibrated Newport 1830-C power meter. The half wave plate was rotated by hand to maximise the power through the polarising beam splitter. The linear polariser was rotated 360˚ by hand and the powers were measured, and their angles were recorded. The calibrated angles with the maximum power at the output of the transmitted and reflected sides of the polarising beam splitter were designated Horizontal and Vertical respectively.

The polarisation angle experiment consisted of the lasers at the QKD transmitter, a linear polariser, and a calibrated Newport 1830-C power meter. Each laser source had output a maximum of 1 nW at the output of the spatial filter. Then the linear polariser was inserted between the spatial filter and the power meter. The linear polariser was rotated 180˚ by hand and the power was measured at 45˚ increments starting from the Horizontal marking. The polarisation angles 45˚, 90˚, 135˚, 180˚ were used as the ideal polarisation references for A, V, D, H respectively. The power of the lasers were maximised when the linear polariser angle

aligned with the laser polarisation. The power of the lasers were minimised when the linear polariser angle was orthogonal with the laser polarisation. The power of each measured angle on the linear polariser was recorded for each laser source. The measured polarisation angles were compared with the calibrated markings on the rotation mount. The calibration markings were equal to the ideal polarisation angles.

Table 16 shows the ideal and measured polarisation angles at the output of the spatial filter. It is shown that the angles are nearly the same and are in agreement. The measured polarisation angles for V, D, and A were within 1 degree of the ideal polarisation angles. The difference between the measured and the ideal polarisation angles must be minimised to ensure the detected photons are measured correctly and end up in the correct SPAD.

Table 16: Ideal and measured polarisation angles for each transmitter basis.

	Polarisation Angle (degrees)	
Polarisation Basis	Ideal	Measured
H	180	180
V	90	89
D	135	134
A	45	46

In this section, the polarisation analysis is limited. A way to improve this section is to perform an experiment for the degree of polarisation on each laser. The degree of polarisation is a measurement of the extent to which the transmitter qubit states are polarised at the output of the spatial filter. A perfectly polarised beam is denoted 1, an unpolarised beam is denoted 0, and a partially polarised beam is between 0 and 1. The degree of polarisation (also known as the visibility V) is [220]

$$V = \frac{I_{max} - I_{min}}{I_{max} + I_{min}} = \frac{I_p}{I_p + I_n} \tag{27}$$

where I_{max} is the maximum intensity of light, I_{min} is the minimum intensity of light, I_p is the intensity of the polarised portion of the light, and I_n is the intensity of 'natural light' or the unpolarised portion of the light.

The degree of polarisation experiment was not performed in this thesis. It is recommended for a more comprehensive analysis on the polarisation of the qubit states and the potential polarisation error (see chapter 6 section 6.1.1). The results of the experiment could provide estimates on the ellipticity of the qubit states which could translate to QBER.

4.4.2 Indistinguishability

The four lasers must be indistinguishable in the temporal, spectral, and spatial domains. If one of these factors is not satisfied, a potential side channel attack can occur on the optical setup. Information about each laser can be distinguished from the differences in temporal pulse widths and amplitudes, spectral laser linewidths, centre wavelengths, and relative intensity, and spatial overlap of the beam profiles.

The spatial filter components were chosen to ensure all output beam profiles were similar. As previously stated in section 4.3.1.3, the output laser beams for H, V, D, A polarisations passed through a common spatial filter with a Ø5 µm pinhole. The spatial filter aligned the laser beams and made the beams spatially indistinguishable.

4.4.2.1 Mutual Information Calculation for Temporal and Wavelength Indistinguishability

Mutual information or information leakage is the amount of information shared between two parties. We define the mutual information between Alice and Bob as [138]

$$I(A:B) = H(A) - H(A|B) \tag{28}$$

where $H(A)$ is the information entropy of Alice on her parameters and $H(A|B)$ is the conditional entropy of Alice based on Bob's measurements. Similarly, we define the mutual information between Alice and Eve as $I(A:E)$ and between Bob and Eve as $I(B:E)$. If $I(A:E)$ or $I(B:E)$ equals zero, this means there is no mutual information or information leaked from the parameters; hence the parameters are indistinguishable to Eve.

For the experiment, the mutual information was calculated by performing a cross-correlation (Y) of the laser parameters for the two lasers in the same basis. The laser parameters used in the cross-correlation analysis were the transmit pulse width and amplitude and the spectral linewidth, centre wavelength, and relative intensity.

Cross-correlation (Y) is given by [272]

$$Y(\Delta s) = \int f^*(s)g(s+\Delta s)ds \tag{29}$$

where Y is defined as the offset of the parameters (i.e. transmit pulse shape and laser spectrum) between the four lasers. The range for Y is between 0 and 1. If $Y(\Delta s = 0) = 1$, the parameters of the source are indistinguishable.

The mutual information leaked to Eve from Alice due to side channel attacks are defined in Eq. (30) – (33) [138]

$$I_{\{H,V\}}(W:E) = 1 - Y_{\{H,V\}} \tag{30}$$

$$I_{\{D,A\}}(W:E) = 1 - Y_{\{D,A\}} \tag{31}$$

$$I_{\{H,V\}}(\wedge:E) = 1 - Y_{\{H,V\}} \tag{32}$$

$$I_{\{D,A\}}(\wedge:E) = 1 - Y_{\{D,A\}} \tag{33}$$

where $I_{\{H,V\}}$ is the information leakage for Horizontal/Vertical basis, $I_{\{D,A\}}$ is the information leakage for the Diagonal/Anti-diagonal basis, $I(W:E)$ is the information leakage of the transmit pulse shape to Eve, $I(\wedge:E)$ is the information leakage of the laser spectrum to Eve, $Y_{\{H,V\}}$ is the cross-correlation between the Horizontal/Vertical basis, and $Y_{\{D,A\}}$ is the cross-correlation between the Diagonal/Anti-diagonal basis.

4.4.2.2 Temporal Indistinguishability Experiment

An experiment was conducted to measure the transmitted pulses of the lasers. The experimental apparatus consisted of the single mode fibre lasers at the QKD transmitter and a New Focus 6 GHz IR detector with single mode fibre input (model 1511). Each laser transmitted a NIM pulse with +0.4 V amplitude and 6 ns FWHM pulse width. The transmitted pulses were measured by directly connecting the single mode fibre lasers to the IR detector. An oscilloscope was used to capture each pulse for each polarisation basis from the IR detector.

The lasers were configured using the controller boards and a configuration file to set each laser bias current and AC input modulation amplitude. The bias current for each laser was set to the minimum threshold to lase. The AC modulation amplitude was fine-tuned to match the maximum heights of the pulses. The ID900 was used to set the repetition rate and the pulse width for the NIM pulses; however these were also limited by the ID900. Consequently, the

transmitter pulse widths were long (6 ns) and had slow rise and fall times at the output of the laser driver.[3] Figure 45 shows a plot of the measured transmitted pulses in voltage vs time, showing the high degree of similarity between the pulses.

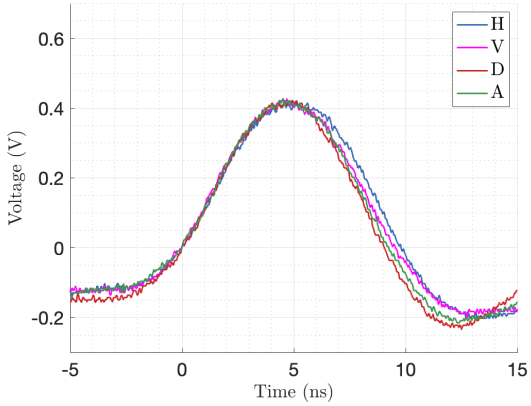


Figure 45: Plot of the measured transmitter pulses in voltage vs time for the four lasers. The measured transmitter pulses show a high degree of similarity between the pulses. The H pulse has a rise time of 4.91 ns and a fall time of 4.05 ns. The V pulse has a rise time of 4.11 ns and a fall time of 3.86 ns. The D pulse has a rise time of 4.25 ns and a fall time of 3.75 ns. The A pulse has a rise time of 4.48 ns and a fall time of 3.68 ns.

The cross-correlation and information leakage were calculated by

$$Y_{\{H,V\}} = 0.9959605 \tag{34}$$

$$Y_{\{D,A\}} = 0.9897801 \tag{35}$$

$$I_{\{H,V\}}(W:E) = 1 - Y_{\{H,V\}} = 4.039 \times 10^{-3} \tag{36}$$

$$I_{\{D,A\}}(W:E) = 1 - Y_{\{D,A\}} = 10.219 \times 10^{-3} \tag{37}$$

The pulse shapes in the H/V basis were indistinguishable due to $I_{\{H,V\}}(W:E) = 4.039 \times 10^{-3}$ bit/pulse. Similarly, the pulse shapes in the D/A basis were indistinguishable due to $I_{\{D,A\}}(W:E) = 10.219 \times 10^{-3}$ bit/pulse. Overall, the mutual information was $I(W:E) \propto 10^{-3}$

[3] A similar pulse width (6.6 ns) was used in a visible light 650 nm free-space BB84 QKD link [121] F. Tang, S. Gao, X. Wang, and B. Zhu, "A novel synchronization scheme for free-space quantum key distribution system," *2011 Asia Communications and Photonics Conference and Exhibition (ACP),* pp. 1-7, 2011, doi: 10.1117/12.917952.

bit/pulse for the measured pulses. Acceptable values for Eq. (36) and (37) were in the orders of magnitude of 10^{-3}. This value was consistent with experimental side channel analyses of a BB84 QKD source in [138] and BB84 QKD source with decoy states in [145]. The BB84 QKD source in [138] used four laser diodes and the BB84 QKD source with decoy states in [145] used eight laser diodes. Both experiments were optimised for temporal indistinguishability. Therefore, the transmitter was robust against a temporal side channel attack. The minimal difference in the pulse shapes ensured all of the lasers operated at the same mean photon number μ.

4.4.2.3 Wavelength Indistinguishability Experiment

An experiment was conducted to measure the spectra of the lasers. The experimental apparatus consisted of the single mode fibre lasers at the QKD transmitter and a calibrated Agilent 86142B optical spectrum analyser with 0.002 nm resolution. Similar to section 4.4.2.2, each laser transmitted a NIM pulse with +0.4 V amplitude and 6 ns FWHM pulse width. The spectra were measured by directly connecting the single mode fibre lasers to the optical spectrum analyser. Figure 46 shows a plot of the measured spectra in relative intensity vs wavelength, showing the high degree of similarity between the spectra.

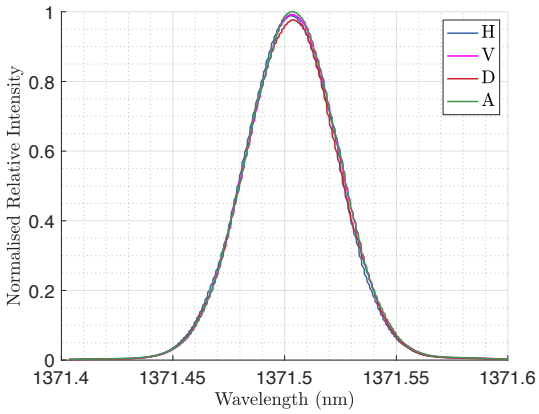


Figure 46: Plot of the measured spectra in normalised relative intensity vs wavelength for the four lasers. The measured spectra show a high degree of similarity between the spectra.

The cross-correlation and information leakage were calculated by

$$Y_{\{H,V\}} = 0.99930393 \tag{38}$$

$$Y_{\{D,A\}} = 0.99964127 \tag{39}$$

$$I_{\{H,V\}}(\wedge: E) = 1 - Y_{\{H,V\}} = 6.96 \times 10^{-4} \tag{40}$$

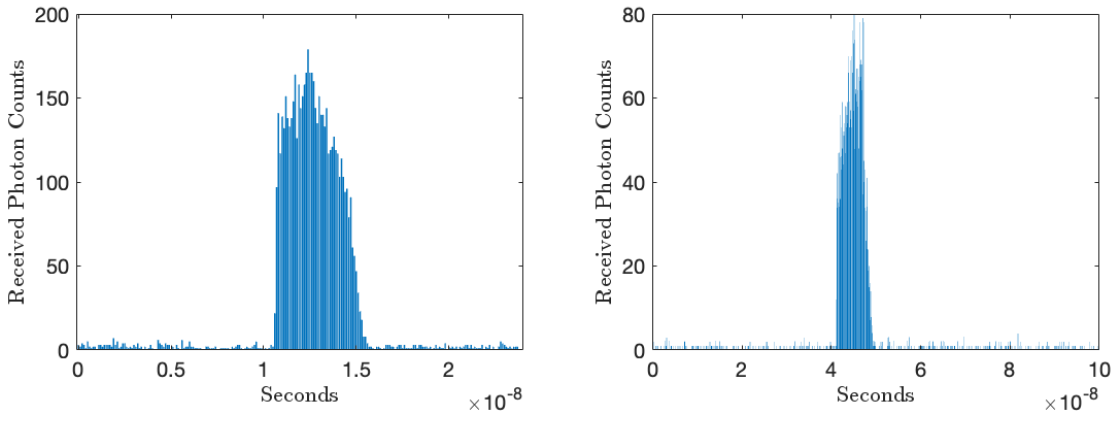
$$I_{\{D,A\}}(\wedge: E) = 1 - Y_{\{D,A\}} = 3.587 \times 10^{-4} \tag{41}$$

The laser spectra in the H/V basis were indistinguishable due to $I_{\{H,V\}}(\wedge: E) = 6.96 \times 10^{-4}$ bit/pulse. Similarly, the laser spectra in the D/A basis were indistinguishable due to $I_{\{D,A\}}(\wedge: E) = 3.587 \times 10^{-4}$ bit/pulse. Overall, the mutual information was $I(\wedge: E) \propto 10^{-4}$ bit/pulse for the measured spectra. Acceptable values for Eq. (40) and (41) were in the orders of magnitude of 10^{-3}. This value was consistent with experimental side channel analyses of a BB84 QKD source in [138] and BB84 QKD source with decoy states in [145]. The BB84 QKD source in [138] used four laser diodes and the BB84 QKD source with decoy states in [145] used eight laser diodes. Both experiments were optimised for wavelength indistinguishability. Therefore, the transmitter was robust against a spectral side channel attack. The minimal difference in the spectra ensures all of the lasers were effectively the same in the spectral domain.

4.4.3 Mean Photon Number

The mean photon number μ was assumed to be 0.1 in the experiment because the mean photon number was not calibrated at the QKD transmitter. Typically, the mean photon number is calibrated for the QKD transmitter by setting a repetition rate for each laser, measuring the total photon counts at the output for each laser, characterising all of the losses in the path lengths of each transmit channel, and ensuring all of the channels output the same photon counts at the output of the non-polarising beam splitter. Then a neutral density filter is placed after the beam

splitter to bring the photon counts down to single photon levels. In this scenario, the mean photon number is calculated as the ratio of the photon counts at the output of the non-polarising beam splitter over the repetition rate. However, the mean photon number was not calibrated prior to attaching the spatial filter to the output of the non-polarising beam splitter. This is evident in the time of arrivals of the received photon counts. Figure 47 shows the time of arrivals for one receiver channel for both repetition rates. Figure 47a shows the time of arrivals from the laser that operated at 41.67 MHz repetition rate. Figure 47b shows the time of arrivals from the laser that operated at 10 MHz repetition rate. These plots are representative examples of receiving photons from one laser that turned on for one second. The widths should be the same for both repetition rates if the mean photon number was calibrated.



(a) (b)

Figure 47: Plot of time of arrivals for one receiver channel. (a) The transmitter operated at 41.67 MHz repetition rate and the width is 6 ns. (b) The transmitter operated at 10 MHz repetition rate and the width is 10 ns.

Consequently, the QKD transmitter was configured such that the output power at the front of the transmitter was measured to be the same across all transmit channels. This ensured the mean photon number was the same across all of the channels because the power levels were the same at the output of the spatial filter. A calibrated Newport 1830-C power meter was used to measure the output power. The linear polariser in front of each laser (‘LP’ in the block diagram

in Figure 38 of section 4.3.1) was manually rotated to reduce the power and number of photons at the output of the transmitter. The output powers for all of the lasers were reduced to the noise floor of the power meter (500 pW). Afterwards, the photon counts were measured more precisely using the ID900 and an idQube SPAD module at the output of each QKD receiver channel. The process of manually rotating the linear polariser for each laser was repeated until the corresponding channels at the QKD receiver were equalised.

4.4.4 Experimental Characterisation of the Receiver

4.4.4.1 Mutual Information Calculation for Polarisation Error

In Figure 43 the non-polarising beam splitter acted as the 50:50 random choice of basis for Bob. One path of the receiver was the H/V basis choice where the polarising beam splitter splits the photon into its 'p' and 's' components. The other path was the D/A basis choice where a half wave plate rotates the photon's polarisation state by 45˚ and then the polarising beam splitter split the photon into its 'p' and 's' components. The received photons were detected in all SPAD modules. However, a clear distinction between the compatible and non-compatible basis resulted in a high extinction ratio. For example, if Alice sends a Horizontal polarisation basis to Bob and assuming Bob chooses the H/V basis, he will notice significantly more photon counts in the H detector compared to the V detector. In addition, the D/A detectors in the other path will show a near 50:50 detection for photon counts. On the contrary, if Alice sends a Diagonal polarisation basis, the half wave plate is used to rotate the photon polarisation to maximise the signal into the Diagonal detector and minimise the signal in the Anti-diagonal detector. The H/V detectors in the other path will show a near 50:50 detection for photon counts.

The polarisations for each basis were not perfect in practice due to imperfect optics or a misalignment in the transmitter setup. In a side channel attack, Eve can extract the information

about the H, V, D, A polarisations sent by Alice if the difference in non-compatible basis or 'crosstalk' is significant. That is, Eve's understanding of the crosstalk matrix and the mismatch in the errors of the non-compatible basis can allow her to guess which polarisations were sent to Bob during the basis reconciliation step in the BB84 protocol.

The equations used in this thesis for the polarisation error analysis are based on the equations found in [138]. This paper experimentally analysed side channels of a BB84 QKD source. The equations used to calculate the mutual information from polarisation error in [138] were modified to reflect the average errors in the crosstalk for the orthogonal basis H/V and D/A. The polarisation error at the transmitter is the error in the non-compatible basis or 'crosstalk' for H/V $(e_{H/V})$ and D/A $(e_{D/A})$ based on the transmitted state. For instance, the polarisation error in the H transmitted state is $(e_{D/A}|H)$ based on the differences in the D and A received states in the crosstalk matrix. Similarly, the polarisation errors for V, D, and A inputs are $(e_{D/A}|V)$, $(e_{H/V}|D)$, and $(e_{H/V}|A)$ respectively. The average of the polarisation errors and the mismatch in the polarisation errors (Δe) are shown in Eq. (42) – (44).

$$e_{D/A,avg} = \frac{1}{2}\left((e_{D/A}|H) + (e_{D/A}|V)\right) \tag{42}$$

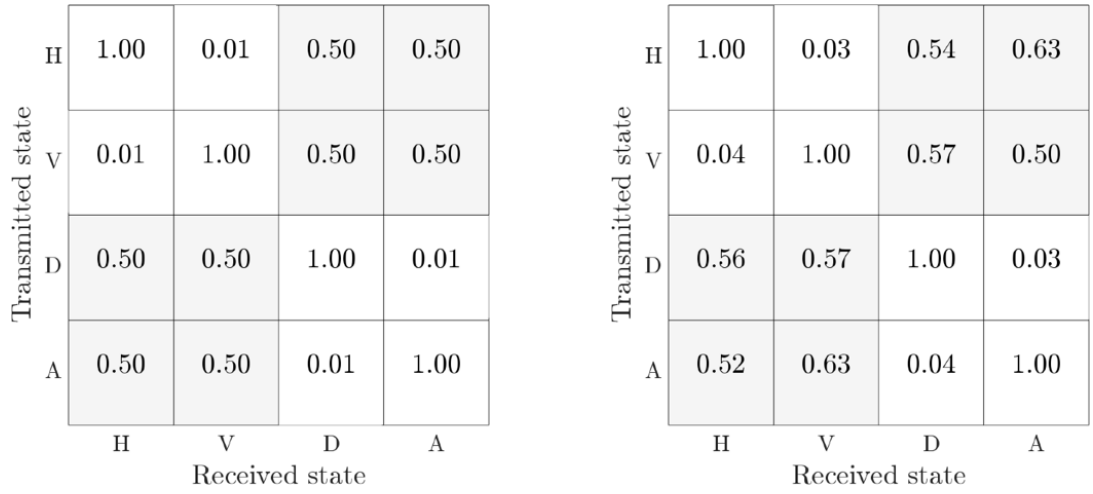
$$e_{H/V,avg} = \frac{1}{2}\left((e_{H/V}|D) + (e_{H/V}|A)\right) \tag{43}$$

$$\Delta e = \left|e_{H/V,avg} - e_{D/A,avg}\right| \tag{44}$$

4.4.4.2 Polarisation Extinction Ratio and Crosstalk Experiment

An experiment was conducted to measure the polarisation extinction ratio and polarisation crosstalk at the QKD receiver. The extinction ratio was the difference between the receiver channels of the compatible basis choice for a transmitted polarisation. For example, for a transmitted H polarisation the extinction ratio was the difference between the H and V receiver channels. The crosstalk was the difference between the receiver channels of the non-compatible

basis choice for a transmitted polarisation. For example, for a transmitted H polarisation the crosstalk was the difference between the D and A receiver channels. The experiment consisted of the QKD transmitter, the QKD receiver, and a calibrated Newport 1830-C power meter. The distance between the transmitter and receiver was 23 cm. The QKD transmitter transmitted 1 nW of optical power (CW) for each polarisation. This value was chosen to ensure it was within the dynamic range of the power meter. The received power was measured for each channel in the QKD receiver at the output of each Thorlabs F280FC-C collimator using a single mode fibre coupled to a Newport 1830-C power meter.



(a) (b)

Figure 48: Normalised extinction ratio and crosstalk matrices for (a) an ideal BB84 receiver and (b) the experimental QKD receiver for each polarisation transmitted with 1 nW of power (CW).

Figure 48 shows the normalised extinction ratio and crosstalk matrices of an ideal BB84 receiver and the experimental QKD receiver in Figure 43. Figure 48a shows the normalised extinction ratio and crosstalk matrix for an ideal BB84 receiver. Figure 48b shows the experimental normalised extinction ratio and crosstalk matrix at the QKD receiver for each polarisation transmitted with 1 nW of power (CW). The measured powers at the receiver for each polarisation state were normalised to the measured power received for the transmitted polarisation state. For instance, in Figure 48b for TX row H, the received powers in RX columns

H, V, D, A were normalised to the received power in RX column H. The same method was used to normalise TX rows V, D, A.

It can be seen in Figure 48b that there was a high extinction ratio in the compatible basis; hence, the intended basis choice is clear. However, there were errors in the non-compatible basis as these are not evenly distributed at 50:50 due to the non-polarising beam splitters and half wave plates. These errors can be exploited in a side channel attack by Eve. Based on the values in Figure 48b, the polarisation errors in the crosstalk were

$$\left(e_{D/A}|H\right) = 0.63 - 0.54 = 0.09 \tag{45}$$

$$\left(e_{D/A}|V\right) = 0.57 - 0.50 = 0.07 \tag{46}$$

$$\left(e_{H/V}|D\right) = 0.57 - 0.56 = 0.01 \tag{47}$$

$$\left(e_{H/V}|A\right) = 0.63 - 0.52 = 0.11 \tag{48}$$

Hence,

$$e_{D/A,avg} = \frac{1}{2}\left(\left(e_{D/A}|H\right) + \left(e_{D/A}|V\right)\right) = 0.08 \tag{49}$$

$$e_{H/V,avg} = \frac{1}{2}\left(\left(e_{H/V}|D\right) + \left(e_{H/V}|A\right)\right) = 0.06 \tag{50}$$

$$\Delta e = \left|e_{H/V,avg} - e_{D/A,avg}\right| = 0.08 - 0.06 = 0.02 \tag{51}$$

The average polarisation error in the D/A crosstalk was $e_{D/A,avg} = 0.08$. The average polarisation error in the H/V crosstalk was $e_{H/V,avg} = 0.06$. The mismatch was $\Delta e = 0.02 = 2 \times 10^{-2}$. The information leaked to Eve from Alice was $I(A:E) \propto \Delta e \propto 10^{-2}$ bit/pulse. This method to equate the amount of information leakage to a direct proportion of the mismatch Δe was used in [138]. The acceptable value for the average polarisation error was in the orders of magnitude of 10^{-2}. This value is consistent with the results from [138] which had an extinction ratio and crosstalk matrix that was nearly ideal. The information leaked from imperfect polarisations can lead to a side channel attack. Eve can use the mismatch in the errors of the non-compatible basis to guess which polarisations are sent to Bob during the basis reconciliation step in the BB84 protocol. However, the mismatch in polarisation errors Δe was

lower than the result in [138] which was $\Delta e = 2.5 \times 10^{-2}$. Therefore, the information leakage to Eve from polarisation error was low. The polarisations generated at the transmitter were approximately aligned to their ideal angles.

4.5 Experimental Methodology

This experiment was a proof of concept for a novel wavelength of operation for indoor free-space QKD links in the presence of ambient light. Figure 49 shows the block diagram of the experimental setup. The free-space QKD link was demonstrated over 23 cm. The link length was chosen due to limited space constraints on the optical bench. The ID900 Time Controller [273] was the central node between Alice and Bob for control of the transmission and reception of the qubits used in the BB84 protocol, data acquisition, and the timing information for Alice's sent qubits and Bob's received qubits for post-processing. The qubit states in the BB84 protocol were represented by the four laser sources for H, V, D, A polarisations. In a realistic QKD system, there is a public channel where Alice and Bob communicate for 1) authentication, 2) time synchronisation of the clock pulses and the gating window, and 3) basis reconciliation, error correction, and privacy amplification. However, a public channel was unnecessary in this proof of concept experiment. It was assumed that Alice and Bob with the ID900 as the central node were all authenticated. The time synchronisation with a gating window, basis reconciliation, error correction, and privacy amplification were achieved during post-processing in Matlab.

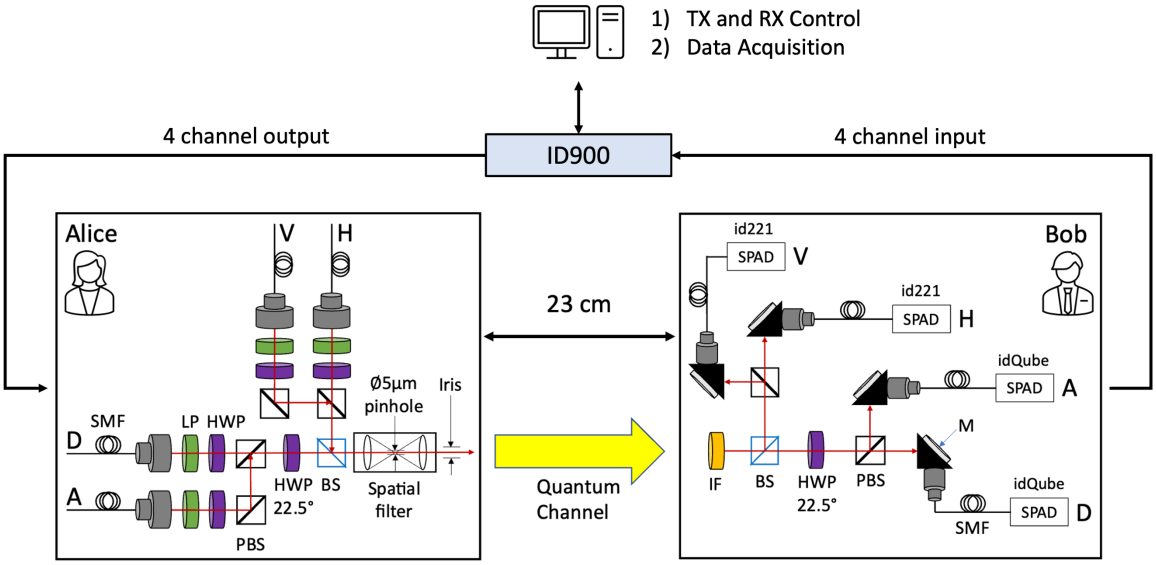


Figure 49: Experimental system block diagram for BB84 free-space QKD system. The terms used are **SMF**: Single Mode Fibre, **LP**: Linear Polariser, **HWP**: Half Wave Plate, **PBS**: Polarising Beam Splitter, **BS**: Beam Splitter, **IF**: Interference Filter, **M**: Mirror, **H**: Horizontal, **V**: Vertical, **D**: Diagonal, **A**: Anti-diagonal, **SPAD**: Single Photon Avalanche Diode. The free-space distance between the transmitter and receiver (23 cm) is shown here for the record.

Four experiments were conducted to show the effect of ambient light on the QKD system. Two experiments were conducted for the QKD system that operated at 41.67 MHz repetition rate with durations of 30 and 60 minutes. The 41.67 MHz repetition rate was the fastest transmit repetition rate for the ID900. This was set by running the ID900 output channels at the shortest period of 24 ns. The other two experiments were conducted for the QKD system that operated at 10 MHz repetition rate with durations of 30 and 60 minutes. The 10 MHz repetition rate was set by running the ID900 output channels at a period of 100 ns. Two repetition rates were used to show the repeatability of the QKD link experiments.

The QKD link was demonstrated under three different ambient light conditions: dark, LED ceiling lighting, and illumination from a halogen lamp (represents sunlight conditions). Darkness was measured with all of the lights off in a laboratory. LED ceiling lighting was measured at 200 lx at the aperture of the receiver using the Amprobe LM-100 lux meter. The

halogen lamp was located 60 cm away from the QKD receiver and pointed directly at the aperture of the receiver. The illumination levels of the halogen lamp were measured at 800 lx at the aperture of the receiver to ensure the same level as measured sunlight at 100k lx between 1351 – 1414 nm (‘Sunny: 100k lx’ in Figure 33). Figure 50 shows the experimental apparatus used in the BB84 free-space QKD experiment.

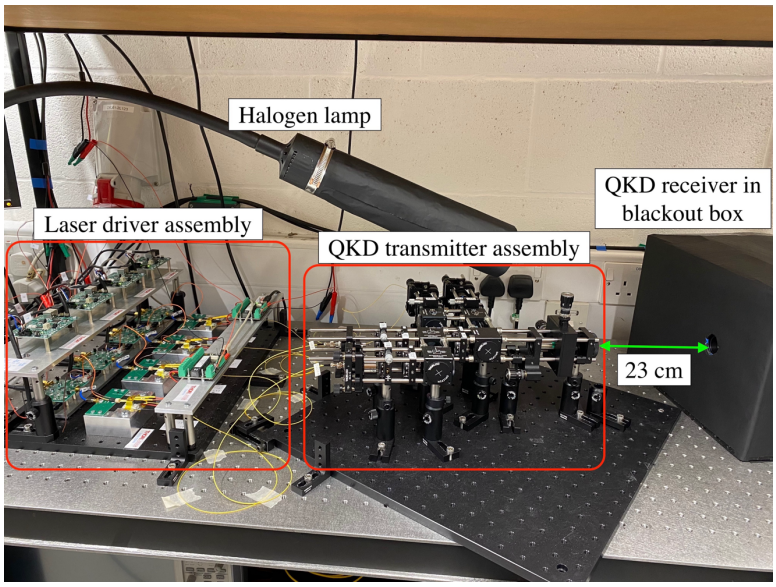


Figure 50: Picture of the experimental apparatus used in the BB84 free-space QKD link experiment. The QKD transmitter (Alice) consisted of the QKD transmitter assembly and laser driver assembly. The QKD receiver (Bob) was inside the blackout box. The ambient light used in the experiment consisted of the LED ceiling lighting (background illumination in the photo) and the halogen lamp. The free-space link distance was 23 cm.

In order to test the effect of ambient light on the QKD system, the QKD receiver was exposed to three ambient light conditions at certain time intervals. Initially, the QKD system operated in complete darkness. Then LED ceiling lighting was turned on and finally the halogen lamp was turned on. In the two ‘30 minute’ experiments, the QKD system was in complete darkness for 10 minutes, next in the presence of LED ceiling lighting for 10 minutes, and finally in the presence of a halogen lamp for 10 minutes. Similarly in the two ‘60 minute’ experiments, the QKD system was in complete darkness for 10 minutes, next in the presence of LED ceiling

lighting for 10 minutes, and the remaining 40 minutes in the presence of a halogen lamp. The QKD system was exposed to a longer duration under the halogen lamp to show the durability and robustness of the QKD system in the presence of sunlight.

4.5.1 Initialisation

At the start of the experiments, the SPAD modules were cooled to reduce the thermal noise which predominantly caused dark counts. The SPAD modules (ID Quantique id221 and idQube) operated in free-running mode at 25 µs dead time and at 10% detection efficiency. The dark counts of the SPAD modules were 500 counts per second on average. SPAD modules that operated in free-running mode do not use a gating window rather the gate signal for the SPAD module was always set to the 'active state'. When a photon was detected, the SPAD module registered the photon count to the ID900 Time Controller, and the diode turned off and was actively quenched during the dead time. This active quench period was shorter than the dead time of the SPAD module. When the dead time was over, the diode was open for photons and the process started again.

The ID900 Time Controller initialised a histogram for each SPAD module for baseline dark counts. The dark counts were recorded in a laboratory with all the lights off and the transmitter was turned off. A histogram was used to determine the probability of a photon detection based on the time of arrival of the photon counts.

4.5.2 Experimental Operation

The ID900 was used to modulate the lasers at the transmitter (Alice) using output channels 1 – 4 which corresponded to Ch 1 – H, Ch 2 – V, Ch 3 – D, Ch 4 – A. The ID900 sent a 6 ns NIM pulse at a period of 24 ns or 100 ns to the laser driver of the chosen polarisation in a repetitive sequence of H, V, D, A. Each laser was turned on for 1 second and then off for 20 seconds such

that the start of the next sequence for the H laser was 84 seconds later. Laser driving patterns using one laser consecutively were not used (i.e. HHHH…). In a practical scenario, the lasers would be driven randomly and one laser may be used consecutively. The consecutive and repeated use of a laser may not allow a laser to reset after each pulse. This leads to variations in pulse intensity and pulse shape with different interpulse delays. Such differences between the pulses could lead to higher QBER and side channel attacks. Therefore, it is important to ensure the same optical characteristics and interpulse delays for each pulse in a practical system.

For each laser in the sequence, the receiver (Bob) registered the photon counts distributed across all of the SPAD modules and sent them to the input channels of the ID900. The photon detections were recorded, timestamped, and displayed in a histogram for each detector. When the compatible basis was used, the intended polarisation received the most photon counts in the corresponding SPAD module and histogram. When the non-compatible basis was used, the number of photon counts should show similar results to Figure 48b (section 4.4.4.2) across the corresponding SPAD modules and histograms. The imbalances and polarisation mismatch in the non-compatible bases were mainly due to the imperfect optical components such as the non-polarising beam splitter and half wave plate at the QKD receiver.

4.5.3 Post-processing

After the duration of the experiments, post-processing was implemented in Matlab to 1) authenticate Alice and Bob, 2) sync the qubits sent by Alice with the measurements made by Bob, 3) use a gating window to temporally filter the received photon counts, 4) compare bases to create the sifted key, and 5) sample the sifted photon counts in 84 second intervals to group them into HVDA sequences. Next, 6) the QBER for each HVDA sequence was calculated to check for any eavesdropping from the quantum channel, and finally 7) the GLLP unconditional secure key rate was calculated for each HVDA sequence using the formulae in section 4.5.3.1.

The GLLP security proof is named after Daniel Gottesman, Hoi-Kwong Lo, Norbert Lutkenhaus, and John Preskill. The authors proved the unconditional security of Quantum Key Distribution using the BB84 protocol with imperfect devices [36]. GLLP uses one-way post-processing such as error correction and privacy amplification [274]. This method determines the unconditional secure key rate at the asymptotic limit. In this thesis, the experiment is a proof of concept to test the system robustness to ambient light and does not consider finite key effects nor the impact of block size. Research into finite key effects for free-space QKD systems can be found in [55, 275-277]. In a practical scenario if each HVDA sequence was within the finite key regime with a sufficient block size, the final secure key length could be divided into 256-bit blocks for composable keys (i.e., usable keys for practical applications like encryption). 256-bits is representative of the key length used in AES encryption and is a reasonable length key in practice.

4.5.3.1 Secure key rate calculation

The secure key rate using GLLP for unconditional security in the asymptotic block size regime [274] is defined as

$$R_{GLLP} \geq q\{-Q_{\mu}H(E_{\mu}) + Q_1[1 - H(e_1)]\} \quad (52)$$

where R_{GLLP} is the GLLP secure key rate (bit/pulse), q is the probability of a basis match, Q_{μ} is the error correction efficiency, $H(z)$ is the binary entropy function, E_{μ} is the QBER, Q_1 is the gain of a single photon state, e_1 is the error rate of a single photon state, and μ is the average number of photons per pulse (mean photon number).

In Eq. (52) and (53) q is calculated by the ratio of sifted qubits with the correct basis over the total number of qubits received by Bob (for the ideal BB84 protocol q = 0.5). After basis reconciliation, N_{μ}^{s} is the number of qubits where Alice and Bob used the same basis. N is the

total number of qubits received by Bob. The secure key rate R_{GLLP} is calculated for each repetitive sequence of HVDA.

$$q = \frac{N_\mu^s}{N} \tag{53}$$

In Eq. (52) and (54) Q_μ is calculated by the ratio of the length of Bob's sifted key where Bob gets detections using the same basis as Alice (K_μ^s) over the number of qubits where Alice and Bob used the same basis (N_μ^s).

$$Q_\mu = \frac{K_\mu^s}{N_\mu^s} \tag{54}$$

In Eq. (52) and (55) $H(z)$ is the binary entropy function with probability z.

$$H(z) = -z\log_2(z) - (1-z)\log_2(1-z) \tag{55}$$

In Eq. (52) and (56) the QBER (E_μ) is the probability that Bob receives a wrong detection in the pulse given Alice and Bob use the same basis. The ratio is the number of wrong qubits in Bob's sifted key (K_μ^{err}) over the length of Bob's sifted key where Bob gets detections using the same basis as Alice (K_μ^s).

$$E_\mu = \frac{K_\mu^{err}}{K_\mu^s} \tag{56}$$

In Eq. (52) and (57) Q_1 is the gain of a single photon state. In Eq. (52) and (58) p_M is the probability of a multi-photon state. In Eq. (52) and (59) e_1 is the error rate of a single photon state.

$$Q_1 = Q_\mu - p_M \tag{57}$$

$$p_M = 1 - (1+\mu)e^{-\mu} \tag{58}$$

$$e_1 = \frac{Q_\mu E_\mu}{Q_1} \tag{59}$$

4.6 Experimental Performance Results for a QKD Link

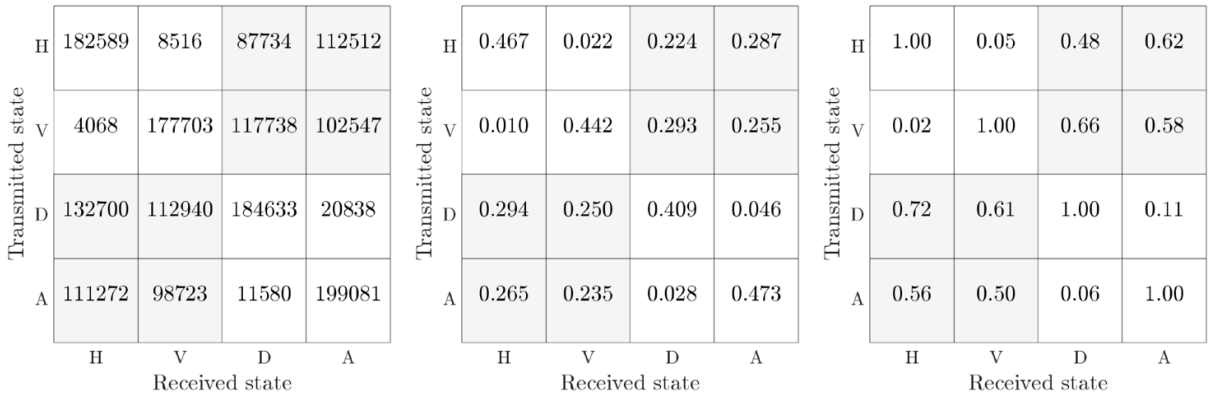
The performance results for the QKD link that operated at 41.67 MHz repetition rate are detailed in this section. These two experiments that ran for 30 and 60 minutes are representative examples of the data collected across all four experiments. Supplemental data for all four experiments can be found in the Appendix. First, the extinction ratio and crosstalk matrices for the QKD link are analysed and the polarisation errors are calculated. Second, the performance results of the two experiments that ran for 30 minutes and 60 minutes are analysed. Lastly, the link budgets for the 30 and 60 minute experiments are analysed.

During the post-processing step, a range of gating windows from 0.2 – 6 ns was used to temporally filter the received photon counts across all four receiver channels for all experiments. The 6 ns gating window was the maximum gating window used because this was the pulse width of the transmitted NIM pulse from the ID900. The results of applying the 6 ns gating window to the 30 and 60 minute experiments are reported in this section. Interestingly, the optimum gating window was 3 ns for all experiments. This achieved a minor improvement in QBER, GLLP secure key rate, and the secure key compared to the 6 ns gating window. However, there is a trade-off between narrowing the gating window and the amount of signal photons. The gating windows that were narrower than 3 ns filtered out more signal than noise. The results using the 3 ns gating window can be found in the Appendix.

4.6.1 Extinction Ratio and Crosstalk Matrix Results

Figure 51 shows the extinction ratio and crosstalk matrices for the QKD system that operated at 41.67 MHz repetition rate for 30 minutes. A 6 ns gating window was used. Figure 51a shows all of the received photon counts for each receiver based on the transmitted state for the entire 30 minutes. Figure 51b shows the ratio of the counts relative to the total received counts based

on the transmitted state. Figure 51c shows the normalised distribution of the counts based on the maximum received counts for the transmitted state in Figure 51a. For example, in row Transmitted state H, the received photon counts in columns Received state H, V, D, A are normalised to the measured photon counts in column Received state H. The same method is used to normalise Transmitted states V, D, A.



(a) (b) (c)

Figure 51: Crosstalk matrices for the 30 minute experiment. Each matrix shows (a) the distribution of received photon counts across 30 minutes, (b) the ratio of received counts in each received state (column) relative to the total received counts per transmitted state (row), and (c) the normalisation of the received states (column) relative to the maximum received counts per transmitted state (row).

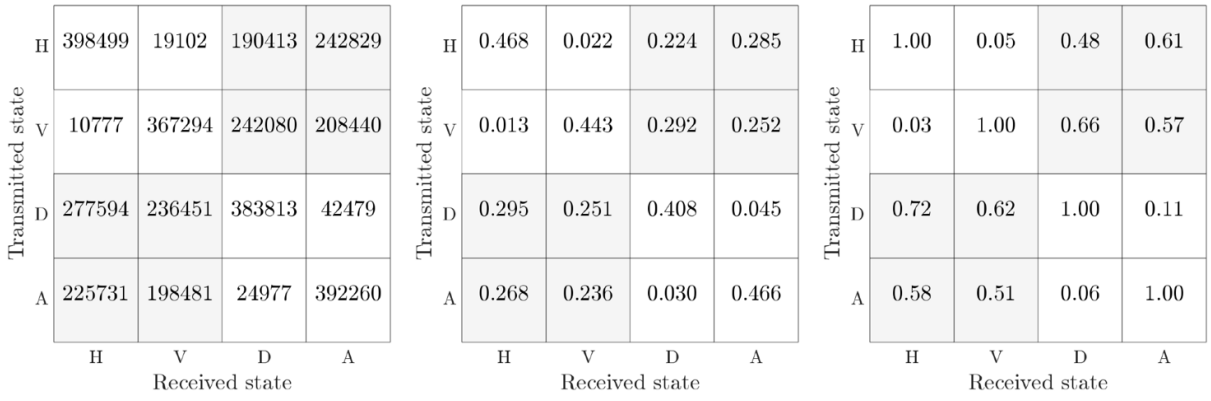
It can be seen in Figure 51c that the compatible basis has a received qubit state that shows a high extinction ratio for the transmitted qubit state at the QKD receiver. In the non-compatible basis, there is increased crosstalk due to imperfect optics such as the non-polarising beam splitters and half wave plates or polarisation misalignment errors. The polarisation errors of the QKD transmitter are calculated by using Eq. (42) – (44) in section 4.4.4.1. Table 17 shows the results of the crosstalk polarisation error calculations.

Table 17: Crosstalk polarisation error calculations for 30 minute experiment

30 min (41.67 MHz, 6 ns)
$(e_{D/A}\|H) = 0.62 - 0.48 = 0.14$
$(e_{D/A}\|V) = 0.66 - 0.58 = 0.08$
$(e_{H/V}\|D) = 0.72 - 0.61 = 0.11$
$(e_{H/V}\|A) = 0.56 - 0.5 = 0.06$
$e_{D/A,avg} = 0.11$
$e_{H/V,avg} = 0.085$
$\Delta e = 0.11 - 0.085 = 0.025$

The average polarisation error in the D/A crosstalk is $e_{D/A,avg} = 0.11$. The average polarisation error in the H/V crosstalk is $e_{H/V,avg} = 0.085$. The mismatch is $\Delta e = 0.025 = 2.5 \times 10^{-2}$. The information leaked to Eve from Alice is $I(A:E) \propto \Delta e \propto 10^{-2}$ bit/pulse. The mismatch Δe from this calculation is the same as the result in [138].

Figure 52 shows the extinction ratio and crosstalk matrices for the QKD system that operated at 41.67 MHz repetition rate for 60 minutes. A 6 ns gating window was used. The post-processing was the same for the 30 minute and 60 minute experiments.



(a) (b) (c)

Figure 52: Crosstalk matrices for the 60 minute experiment. Each matrix shows (a) the distribution of received photon counts across 60 minutes, (b) the ratio of received counts in each received state (column) relative to the total received counts per transmitted state (row), and (c) the normalisation of the received states (column) relative to the maximum received counts per transmitted state (row).

Table 18: Crosstalk polarisation error calculations for 60 minute experiment

60 min (41.67 MHz, 6 ns)
$(e_{D/A}\|H) = 0.61 - 0.48 = 0.13$
$(e_{D/A}\|V) = 0.66 - 0.57 = 0.09$
$(e_{H/V}\|D) = 0.72 - 0.62 = 0.1$
$(e_{H/V}\|A) = 0.58 - 0.51 = 0.07$
$e_{D/A,avg} = 0.11$
$e_{H/V,avg} = 0.085$
$\Delta e = 0.11 - 0.085 = 0.025$

Table 18 shows the results of the crosstalk polarisation error calculations. It can be seen that the average polarisation error in the D/A crosstalk ($e_{D/A,avg}$), the average polarisation error in the H/V crosstalk ($e_{H/V,avg}$), mismatch (Δe), and the information leaked to Eve from Alice are the same as that of the 30 minute experiment. This suggests that the QKD system can operate with minimal polarisation error and information leakage for at least 40 minutes under the illumination of the halogen lamp. Individual analysis of the polarisation error for the different ambient light scenarios can be found in the Appendix.

4.6.2 Experimental Performance Results for 30 Minute Experiment

The ambient light was incorporated into the experiment at certain time intervals to show its effect on the noise induced by ambient light at the QKD receiver. In the 30 minute experiment, the QKD system was under 10 minutes of darkness, followed by 10 minutes of LED ceiling lighting (200 lx at the aperture of the receiver), and then 10 minutes of a halogen lamp pointed directly at the aperture of the receiver (800 lx at the aperture of the receiver). In this section, we reported and analysed the performance results for the experiment that operated at repetition rate 41.67 MHz only. This was a representative example of the QKD link performance for 30 minutes. Supplemental data of all of the 30 minute experiments can be found in the Appendix.

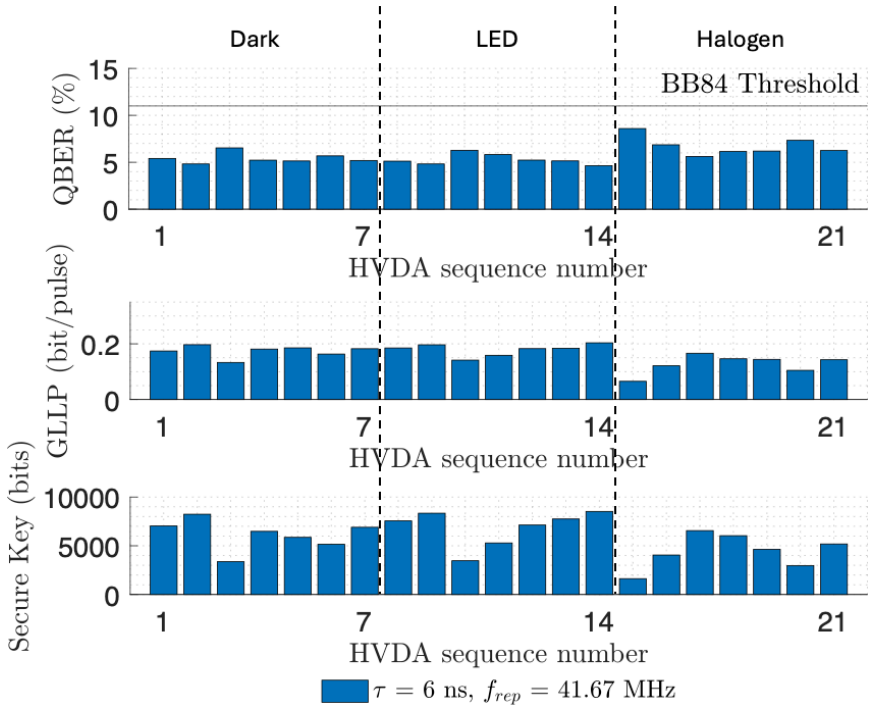


Figure 53: Plot of the results for the 30 minute experiment. The experiment ran for 30 minutes under ambient light conditions: (a) 10 minutes in darkness, (b) 10 minutes under LED lighting, and (c) 10 minutes under a halogen lamp. This is equivalent to 7 HVDA sequences in darkness, 7 sequences under LED lighting, and 7 sequences under halogen lamp. Each iteration in the experiment (1 HVDA sequence) was sampled at 84 seconds. The QBER, GLLP secure key rate, and the number of secure key bits were calculated for each HVDA sequence.

Figure 53 shows a plot of the results of the QKD system that operated at 41.67 MHz repetition rate for 30 minutes under darkness and illumination from LED lighting and halogen lamp. A 6 ns gating window was used in the post-processing. The effect of ambient light on the QBER, GLLP secure key rate, and the secure key are shown over time. Table 19 shows the statistical analysis of the experiment for the entire 30 minutes and individual ambient light scenarios.

Table 19: Statistical analysis for the 30 minute experiment

$f_{rep} = 41.67$ MHz, $\tau = 6$ ns	Total (30 min)	Dark (10 min)	LED (10 min)	Halogen (10 min)
Total signal counts K_μ^{sig}	744,006	244,263	263,945	235,798
Total error counts K_μ^{err}	45,002	13,849	14,517	16,636
Total counts in sifted basis $K_\mu^s = K_\mu^{sig} + K_\mu^{err}$	789,008	258,112	278,462	252,434
Average QBER (%) $E_{\mu,avg}$	5.81%	5.43%	5.29%	6.71%
Average GLLP (bit/pulse) $R_{GLLP,avg}$	0.16	0.174	0.179	0.127
Average error counts $\mu_{err} = E_{\mu,avg} \times K_\mu^{sig}$	43,227	13,264	13,963	15,822
Standard deviation of error counts $\sigma_{err} = \sqrt{\mu_{err}}$	208	115	118	126
Fluctuation in QBER (%) $\frac{\sigma_{err}}{K_\mu^{sig}} \times 100$	0.028%	0.047%	0.045%	0.053%
Total secure key bits $K_{secure} = R_{GLLP,avg} \times K_\mu^{sig}$	119,041	42,502	47,246	29,946

The average QBER is below the BB84 threshold for all three ambient light scenarios as shown in Table 19. The LED ceiling lighting at 200 lx had negligible effect on the QBER. The performance under the LED lighting was similar to the performance in the dark. The average QBER at the transition between the LED lighting and the halogen lamp increased by 1.42%. However, the average QBER at 6.71% under the halogen lamp is comparable to the performance in the dark and under the LED lighting. Hence, the effect of the halogen lamp on the QKD link performance is minimal.

It was assumed there was 0 dB link loss in the experiment due to the controlled laboratory environment and the short distance between the transmitter and the receiver. Also, it was assumed that the component losses inside the QKD receiver were 'trusted' losses (i.e. Eve did not have access to the QKD receiver). Based on these assumptions, we could distil a key with a fair sampling of the HVDA sequence bits. Therefore, the 119,041 total secure key bits in Table 19 could be divided up into 465 256-bit composable keys for encryption. Table 20 shows the link budget for the 30 minute experiment.

Table 20: Link budget analysis for 30 minute experiment

Number of HVDA sequences	7		
Repetition rate (assume one photon per pulse)	41.67×10^6		
Number of transmitter channels	4		
Total signal photons	**1,166,760,000**		
	Dark	**LED**	**Halogen**
Total received counts from transmitted H	123,606	139,852	127,893
Total received counts from transmitted V	135,593	138,886	127,577
Total received counts from transmitted D	147,041	162,153	141,917
Total received counts from transmitted A	138,510	147,274	134,872
Total received counts	**544,750**	**588,165**	**532,259**
Average dark counts per detector	500	500	500
Average dark counts across 4 detectors in one HVDA sequence	2,000	2,000	2,000
Average counts from LED lighting per detector	-	0	-
Average counts from LED lighting across 4 detectors in one HVDA sequence	-	0	-
Average counts from halogen lamp per detector	-	-	300
Average counts from halogen lamp across 4 detectors in one HVDA sequence	-	-	1,200
Average counts from noise sources per transmitted state in 7 HVDA sequences	14,000	14,000	22,400
Total counts from noise sources across all 4 transmitted states	56,000	56,000	89,600
Estimated total received signal counts	**488,750**	**532,165**	**442,659**
Total loss (ratio of received signal counts / transmitted signal photons)	4.19×10^{-4}	4.56×10^{-4}	3.79×10^{-4}
Total loss in dB	33.8 dB	33.4 dB	34.2 dB
Channel loss in dB	0 dB	0 dB	0 dB
Average transmittance across all 4 receiver channels	0.0064	0.0064	0.0064
Average receiver loss in dB	21.9 dB	21.9 dB	21.9 dB
Total loss – Average receiver loss in dB	**11.9 dB**	**11.5 dB**	**12.3 dB**
Estimated mean photon number	0.065	-	-

It can be seen in Table 20 that the estimated total received signal counts are similar across all three ambient light scenarios. Consequently, the total loss was also similar across all three ambient light scenarios. There was a maximum difference of 0.8 dB loss between the LED lighting and halogen scenarios. This small difference suggests the halogen lamp had a minor effect on the QKD link. In addition, this link budget shows that the total estimated internal losses at the receiver was 21.9 dB. Based on the experimental data, the link loss in the dark scenario was estimated to be 33.8 dB. Assuming the channel loss was 0 dB, the mean photon number can be estimated by calculating the difference between the total loss and the average loss. In this case, the estimated mean photon number is 0.065.

4.6.3 Experimental Performance Results for 60 Minute Experiment

The purpose of running the QKD system for 60 minutes was to show the robustness of the system under the halogen lamp for a longer duration of time. This experiment was also used to show that the QKD system could reproduce similar results with the 30 minute experiment. In the 60 minute experiment, the QKD system was under 10 minutes of darkness, followed by 10 minutes of LED ceiling lighting (200 lx at the aperture of the receiver), and then 40 minutes of a halogen lamp pointed directly at the aperture of the receiver (800 lx at the aperture of the receiver). Similar to the previous section, we reported and analysed the performance results for the experiment that operated at repetition rate 41.67 MHz only. This was a representative example of the QKD link performance for 60 minutes. Supplemental data of all of the 60 minute experiments can be found in the Appendix.

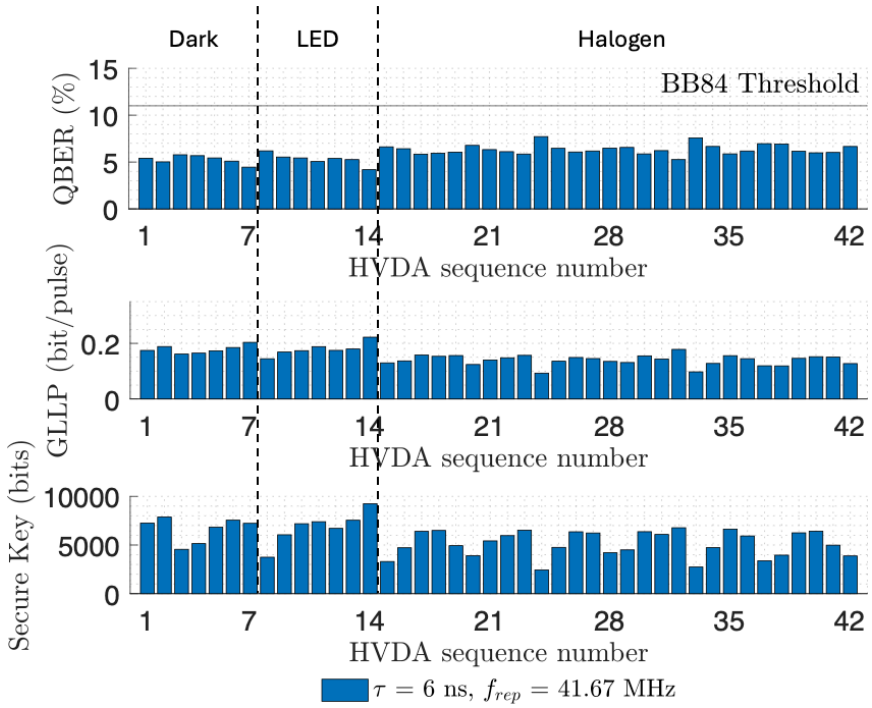


Figure 54: Plot of the results for the 60 minute experiment. The experiment ran for 60 minutes under ambient light conditions: (a) 10 minutes in darkness, (b) 10 minutes under LED lighting, and (c) 40 minutes under a halogen lamp. This is equivalent to 7 HVDA sequences in darkness, 7 sequences under LED lighting, and 28 sequences under halogen lamp. Each iteration in the experiment (1 HVDA sequence) was sampled at 84 seconds. The QBER, GLLP secure key rate, and the number of secure key bits were calculated for each HVDA sequence.

Figure 54 shows a plot of the results of the QKD system that operated at 41.67 MHz repetition rate for 60 minutes under darkness and illumination from LED lighting and halogen lamp. A 6 ns gating window was used in the post-processing. The effect of ambient light on the QBER, GLLP secure key rate, and the secure key are shown over time. Table 21 shows the statistical analysis of the experiment for the entire 60 minutes and individual ambient light scenarios.

Table 21: Statistical analysis for the 60 minute experiment

$f_{rep} = 41.67$ MHz, $\tau = 6$ ns	Total (60 min)	Dark (10 min)	LED (10 min)	Halogen (40 min)
Total signal counts K_μ^{sig}	1,541,866	258,458	264,405	1,019,003
Total error counts K_μ^{err}	97,335	14,303	14,608	68,424
Total counts in sifted basis $K_\mu^s = K_\mu^{sig} + K_\mu^{err}$	1,639,201	272,761	279,013	1,087,427
Average QBER (%) $E_{\mu,avg}$	5.99%	5.27%	5.29%	6.35%
Average GLLP (bit/pulse) $R_{GLLP,avg}$	0.153	0.179	0.179	0.14
Average error counts $\mu_{err} = E_{\mu,avg} \times K_\mu^{sig}$	92,358	13,621	13,987	64,707
Standard deviation of error counts $\sigma_{err} = \sqrt{\mu_{err}}$	304	117	118	254
Fluctuation in QBER (%) $\frac{\sigma_{err}}{K_\mu^{sig}} \times 100$	0.02%	0.045%	0.045%	0.025%
Total secure key bits $K_{secure} = R_{GLLP,avg} \times K_\mu^{sig}$	235,906	46,264	47,329	142,660

It can be seen in Table 21 that the average QBER was still below the BB84 threshold for all three ambient light scenarios. The LED lighting had a negligible effect on the QKD link and was comparable to the system in the dark. The average QBER for the halogen scenario increased by 1.06% from the LED lighting scenario. The duration under the illumination of the halogen lamp was 40 minutes. The effect of the halogen lamp on the QKD link performance was still minimal with an average QBER of 6.35%. These performance results are consistent with the results of the 30 minute experiment. Both experiments have similar average QBER for all three ambient light scenarios.

Similar to the 30 minute experiment, we could distil a key with a fair sampling of the HVDA sequence bits. Therefore, the 235,906 total secure key bits in Table 21 could be divided up into 921 256-bit composable keys for encryption. Table 22 shows the link budget for the 60 minute experiment.

Table 22: Link budget analysis for the 60 minute experiment

Number of HVDA sequences	7		
Repetition rate (assume one photon per pulse)	41.67×10^6		
Number of transmitter channels	4		
Total signal photons	**1,166,760,000**		
	Dark	**LED**	**Halogen (1/4 total received counts)**
Total received counts from transmitted H	147,075	163,652	135,029
Total received counts from transmitted V	140,105	134,808	138,420
Total received counts from transmitted D	165,043	162,065	153,308
Total received counts from transmitted A	126,860	129,565	146,257
Total received counts	**579,083**	**590,090**	**573,014**
Average dark counts per detector	500	500	500
Average dark counts across 4 detectors in one HVDA sequence	2,000	2,000	2,000
Average counts from LED lighting per detector	-	0	-
Average counts from LED lighting across 4 detectors in one HVDA sequence	-	0	-
Average counts from halogen lamp per detector	-	-	300
Average counts from halogen lamp across 4 detectors in one HVDA sequence	-	-	1,200
Average counts from noise sources per transmitted state in 7 HVDA sequences	14,000	14,000	22,400
Total counts from noise sources across all 4 transmitted states	56,000	56,000	89,600
Estimated total received signal counts	**523,083**	**534,090**	**483,414**
Total loss (ratio of received signal counts / transmitted signal photons)	4.48×10^{-4}	4.58×10^{-4}	4.14×10^{-4}
Total loss in dB	33.5 dB	33.4 dB	33.8 dB
Channel loss in dB	0 dB	0 dB	0 dB
Average transmittance across all 4 receiver channels	0.0064	0.0064	0.0064
Average receiver loss in dB	21.9 dB	21.9 dB	21.9 dB
Total loss – Average receiver loss in dB	**11.6 dB**	**11.5 dB**	**11.9 dB**
Estimated mean photon number	0.069	-	-

The QKD link was under the halogen lamp for 4x longer than the dark or LED lighting scenario. Hence, the halogen lamp column in Table 22 used 25% of the total received counts in the dataset for comparison with the dark and LED lighting scenarios. The total received signal counts were similar across all three ambient light scenarios as shown in Table 22. There was a maximum difference of 0.4 dB loss between the LED lighting and halogen scenarios. This suggests the effect of the halogen lamp was still minimal on the QKD link performance. The calculation of the mean photon number was also similar to the estimate from the 30 minute experiment.

Overall, the performance results from the two experiments were consistent and showed that the QKD link performance was robust in the presence of the halogen lamp.

4.7 Discussions and Observations

The statistics shown in Table 19 and Table 21 for each interval suggested that the QKD system was robust under illumination from the LED ceiling lighting and the halogen lamp. The effect from LED lighting was effectively the same as the QKD link in the dark. The effect from the halogen lamp also had minimal effect on the QBER, GLLP secure key rate, and the secure key. The average QBER under the halogen lamp in 10 and 40 minutes was approximately 6.53%. This suggests that a QKD link can operate in direct sunlight at 100k lx while maintaining a QBER below the BB84 threshold for at least 40 minutes.

The experimental results showed that a QKD system operating with a wavelength between 1351 – 1414 nm can perform well under conditions that resemble outdoor direct sunlight [265]. Wavelengths within 1351 – 1414 nm are suited for all QKD protocols and not restricted to BB84. Also, wavelength is one key parameter in the design process of a free-space QKD system. The narrow field of view at the receiver was another key parameter to mitigate the noise caused by ambient light. In this thesis, the QKD receiver utilised a single mode fibre and collimator which narrowed the field of view of the receiver to approximately 0.1˚. This narrow field of view helped enable the performance of the QKD system. Furthermore, the choice of wavelength around 1370 nm may be a more cost-effective design option in practical applications rather than engineering a spatial filter to narrow the field of view.

4.8 Summary

In this chapter, we reported the demonstration of a static line-of-sight free-space QKD link using the BB84 protocol with a centre wavelength of 1371.5 nm in the presence of ambient light. The QKD link distance was 23 cm. The QKD system was tested under three lighting conditions: complete darkness, LED ceiling lighting, and a halogen lamp. The halogen lamp was used as an analogue to outdoor sunlight around 1370 nm. The QKD links were operated at two repetition rates and were conducted for 30 minute and 60 minute durations. The experimental results reported in this chapter showed the QKD system performed well with minimal interference from the LED lighting and the halogen lamp. The QKD link under the LED lighting was effectively the same as operating the link in the dark. The QKD link achieved an average QBER of 6.35% under the illumination from the halogen lamp for at least 40 minutes. Overall, the QKD system at 1371.5 nm worked and performed well under the halogen lamp and this result can extend to outdoor applications for short range links and indoor environments illuminated by ambient light. The QKD system at 1371.5 nm is robust to ambient light and to the author's knowledge, the first of its kind.

Chapter 5 Digital Micromirror Device as part of the QKD Transmitter

In this chapter, we investigate the use of a digital micromirror device (DMD) as part of the quantum transmitter. A DMD is a device typically used in projection displays that can direct light to separate areas as a means to spatially modulate illumination, creating images. A series of tests were conducted to investigate the potential of the DMD to direct single photons to a quantum receiver. The design parameters and application of a DMD as part of the pointing, acquisition, and tracking system are discussed.

5.1 Beam Steering for Indoor Free-space QKD Links

In the previous chapter a BB84 free-space QKD system was demonstrated for a short distance (23 cm) for a LOS static system under ambient light. A more practical scenario is to utilise the system at longer distances with a dynamic tracking element. The tracking system can be integrated into the transmitter in order to direct the QKD signal to a receiver on a desk within a room. An indoor free-space QKD link requires beam steering to direct light from a QKD transmitter to a QKD receiver. Figure 55 shows the indoor free-space QKD link diagram first shown in Figure 4 from section 2.3 for convenience.

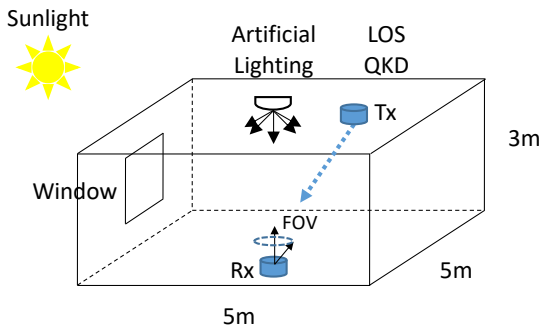


Figure 55. Indoor free-space QKD link in the presence of artificial lighting and sunlight. This diagram is repeated for convenience.

In the room, it is assumed the QKD receiver exhibits nomadic behaviour, i.e. the QKD receiver moves to a desired location within the room and then the QKD receiver stops and establishes a communications link with the QKD transmitter. As the QKD links are narrow beam, some form of beam steering is required to enable the nomadic link. The links would not work without tracking and pointing.

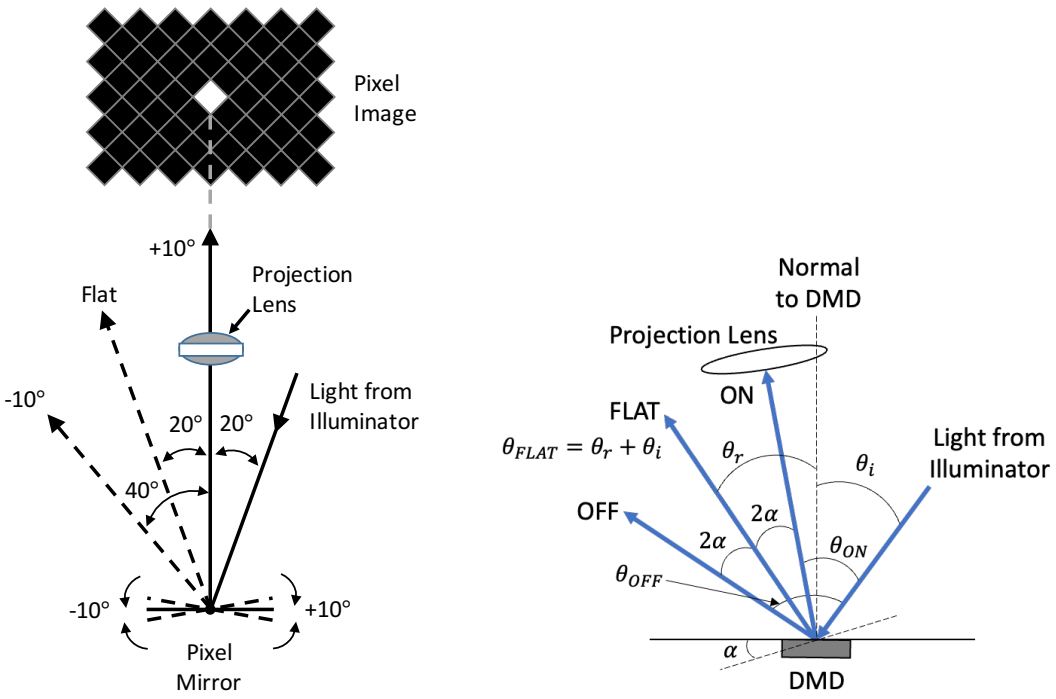
Typically, indoor free-space optical (FSO) links use fast steering mirrors (FSM) for beam steering to direct the light from a transmitter to a receiver [278]. FSMs used in FSO links are usually categorised based on actuator type: mechanical actuator and micro-electromechanical systems (MEMS). A mechanical FSM uses a voice-coil actuator which is a magnetic coil that sits close to the mirror surface. The magnetic coil moves the mirror with a push or pull effect when current flows through the coil. The mirror can tip and tilt to perform two-dimensional axis scanning. The mirrors use a position feedback control system to control and stabilise the angle of the mirror. Mirror sizes of mechanical FSMs are typically larger than MEMS mirrors and offer a wider deflection angle. FSO experiments using mechanical FSMs were reported in [103, 168-175, 279]. An example of an FSM is made by Optotune. The Optotune devices are mechanical FSMs that have a large mirror surface (10 or 15 mm) with a large deflection angle (25˚ – 50˚ full angle) and offer speeds from 20 – 250 Hz [280]. A pair of Optotune mirrors (MR-15-30-G) were used for beam steering in a free-space COW-QKD experiment in [103].

MEMS mirrors are typically made of silicon and etched using the same technology and processes as CMOS semiconductors. A MEMS mirror is controlled by electrostatic actuators beneath the mirror. The actuator tilts the MEMS mirror when a voltage is applied to the actuator. The fabrication process enables a MEMS mirror to be much smaller than a mechanical FSM. An advantage of the smaller size is increased speed in position feedback and beam steering. Larger mirrors have to overcome higher inertia which leads to slower speeds. FSO

experiments using MEMS mirrors were reported in [281-283]. An example of a MEMS mirror is made by Mirrorcle Technologies. The Mirrorcle devices are MEMS mirrors that have a smaller mirror surface (0.8 – 7.5 mm) with a narrower deflection angle (up to 32˚ full angle) but offer much faster speeds (up to 3.6 kHz) [284]. A pair of Mirrorcle mirrors with Ø4.2 mm were used for beam steering in a free-space handheld QKD system in [55].

5.2 Digital Micromirror Device

A digital micromirror device (DMD) [285] is a type of MEMS device that contains a large array of micromirrors on an integrated circuit. A DMD is a cost-effective, commercial, and practical beam steering device that is widely used in projectors incorporating Texas Instruments Digital Light Processing (DLP) technology [286]. Figure 56 shows the DMD optical switching principle. A DMD is a type of amplitude-only spatial light modulator where each micromirror has 3 states: Flat, On ($+10^{\circ}$), and Off (-10°). Beneath each micromirror is a torsion hinge that, when a voltage is applied, controls its state. With no voltage applied to the DMD, the micromirror is in a parked, flat position. With voltage applied, the micromirror can pivot to an On or Off position effectively directing light to display an image.



(a) (b)

Figure 56: DMD optical switching principle. (a) The micromirror (pixel) has three states: Flat, On (+10˚) and Off (–10˚). Light from the Flat and Off states are reflected away from the projection lens. Light reflected from the On state displays a pixel image through the projection lens [286]. (b) A diagram of the angles of the three states relative to the illuminator. The angles in the diagram are: θ_i is the incident angle with respect to the normal of the DMD, θ_r is the angle of the reflection, α is the tilt angle of the micromirror, θ_{ON} is the angle of the On state, θ_{FLAT} is the angle of the Flat state, θ_{OFF} is the angle of the Off state.

In Figure 56b the angles for the three states are based on Eq. (60) – (62) where the angle of reflection equals the incident angle ($\theta_r = \theta_i$) and α is the tilt angle of the micromirror.

$$\theta_{FLAT} = \theta_r + \theta_i = 2\theta_i \tag{60}$$

$$\theta_{ON} = \theta_{FLAT} - 2\alpha = 2(\theta_i - \alpha) \tag{61}$$

$$\theta_{OFF} = \theta_{FLAT} + 2\alpha = 2(\theta_i + \alpha) \tag{62}$$

An example of a projector with a DMD is the Texas Instruments Lightcrafter 4500 (DLPLCR4500EVM [287]). Figure 57 shows the internal setup of the Lightcrafter 4500 [288]. The full angle steering capability of a DMD depends on the optical setup of the projector. The Lightcrafter 4500 projector has a steering capability of up to 45˚ full angle.

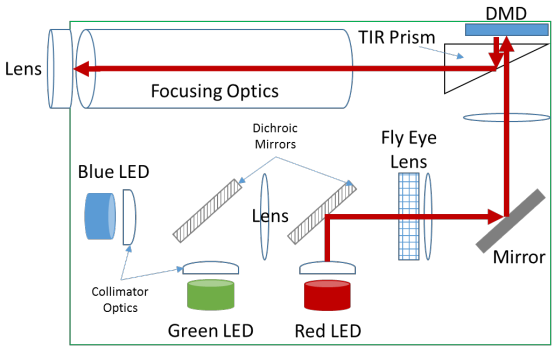


Figure 57: Texas Instruments Lightcrafter 4500 internal layout [288]. The light path for the red illumination is shown. A similar path is taken by other colours.

The DMD (DLP4500 [289]) used in the Lightcrafter 4500 has 912 columns x 1140 rows of micromirrors with 7.6 µm pitch. This version of DMD has mirrors that tilt ±12 degrees. The DLP4500 can operate each micromirror individually from 120 – 4225 Hz. The individual control of the micromirrors enables a DMD to direct light to separate areas of the projection display simultaneously. It can be seen in Figure 56a that a DMD can use one micromirror for illumination instead of all of the micromirrors. Hence, a DMD is considered a high signal loss device. However, the QKD transmitter can tolerate high signal loss because the QKD transmitter only has to transmit a single photon. Therefore, a DMD has the potential to be used in a free-space BB84 QKD system at the transmitter. A DMD was used at the transmitter in two experiments with a He-Ne laser source and Spatial Light Modulator (SLM) for free-space orbital angular momentum (OAM) communications for QKD [241, 290]. OAM is a type of spatial mode encoding using binary holograms. In [290] an initial experiment using a He-Ne laser source and a DMD to create OAM spatial modes was demonstrated. A computer was used to load three different spatial modes onto the DMD. The DMD was used to generate and

separate the different OAM modes at 4 kHz refresh rate (the micromirror switching limit of the DMD in the paper). The conclusions of the experiment showed the intensity profiles and the 'On state' pulse durations of each OAM mode that was measured. The work in [241] was a proof of principle experiment with high dimensional QKD using OAM spatial modes. The experiment built upon the work in [290] using the He-Ne laser source. The experiment consisted of one DMD at the QKD transmitter and two phase-only SLMs at the QKD receiver. A computer loaded seven different OAM spatial modes onto the DMD. The SLMs were used for phase corrections of the received holograms. The conclusion is a high dimensional QKD system is feasible using the transverse structure of light. This allowed for more than 1 bit per photon. Also, multi-level QKD systems can increase the information capacity of a QKD link and can be more resilient against intercept and resend attacks.

5.3 QKD Transmitter Requirements

For an indoor QKD link, the QKD transmitter should be able to effectively send single photons to a QKD receiver anywhere within the desired coverage area. The DMD as part of the QKD transmitter should satisfy four requirements:

1. Uniform illumination of the transmitted signal within a coverage area.
    a. The QKD transmitter should illuminate the coverage area such that the transmitted QKD signal is uniform everywhere within the coverage area.
2. Constant and time-invariant transmitted signal.
    a. The transmitted QKD signal should remain constant over the time period of operation. This requires the DMD micromirrors to hold their state within the gate window of operation for the transmitter (i.e. nanoseconds).
3. Linearity in choosing the number of pixels for illumination.

a. The ability to control a precise number of DMD micromirrors to illuminate the target area. The DMD is a device with high signal loss and therefore may need more than one pixel to send single photons.

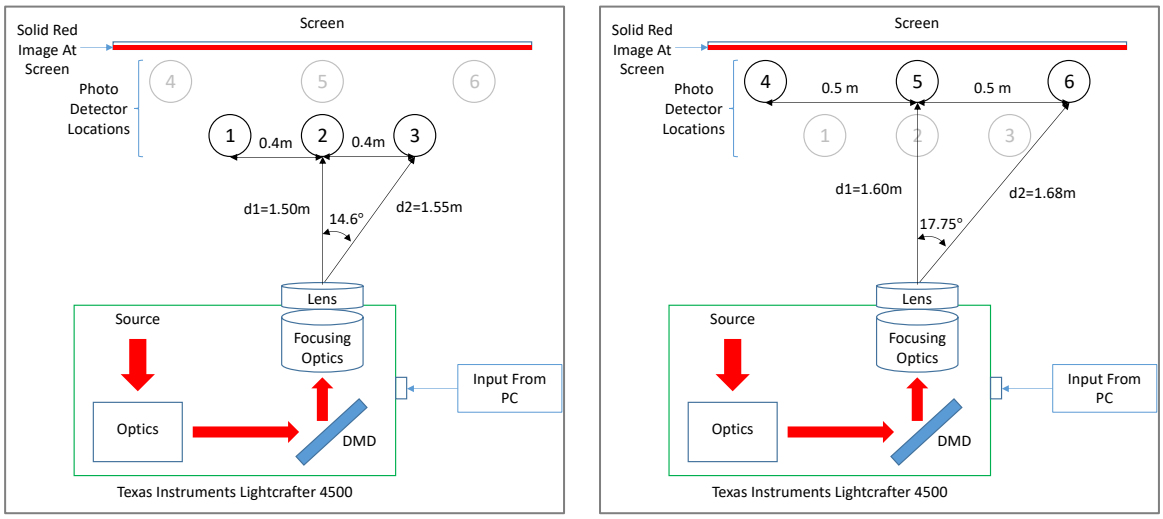
4. Polarisation maintaining.
    a. BB84 and other polarisation-based QKD protocols require the polarisation of the qubit states be precise. The polarisation of the qubits should be maintained after reflection off the DMD surface.

5.4 Feasibility Tests for DMD as QKD Transmitter

A set of experiments were undertaken to test the feasibility of integrating a DMD as part of the QKD transmitter. The experiments were conducted with a Texas Instruments Lightcrafter 4500. The Lightcrafter 4500 uses pulse width modulation (PWM) from the red, green, and blue LED sources in Figure 57 to control the brightness of each micromirror. In Figure 57 the fly eye lens uniformly distributes light over the DMD micromirrors. This makes the DMD an effective homogeneous illuminator.

5.4.1 Uniform Illumination Test

The aim of the experiment is to test whether the Lightcrafter 4500 illuminates a coverage area with uniform intensity. Figure 58 shows the experimental setup of the Lightcrafter 4500 and the photo detector locations in front of a screen.



(a) (b)

Figure 58: Experimental setup diagram of Texas Instruments Lightcrafter 4500 projecting a solid red image onto a screen. (a) The photo detector measurements are made at locations 1 – 3. (b) The photo detector measurements are made at locations 4 – 6. All of the locations are on the optical bench. The corners of the screen are not used for detector measurements.

The experimental apparatus consists of the Lightcrafter 4500, a desktop computer, a 1 MHz bandwidth photo detector with Ø1 cm collection area, and an Agilent Technologies MSO6104A oscilloscope. The Lightcrafter 4500 is connected to a desktop computer and used as an extended monitor display. The red LED is chosen out of the three sources in the Lightcrafter 4500 for this experiment. A solid red image is displayed using the red LED at 50% PWM. The waveform is measured with a 1 MHz bandwidth photo detector with Ø1 cm collection area. The 1 MHz photo detector is sufficient to measure the period of the On states of the DMD. The photo detector is connected to an Agilent Technologies MSO6104A oscilloscope. The photo detector is moved to locations 1 through 6 to take measurements. All of the measurement positions are located on the optical bench and the corners of the screen are not used. This ensures a steady measurement without hand vibrations and enables reliable and repeatable measurements. At each location, the photo detector is orientated in the direction of the Lightcrafter 4500 to maximise the received signal.

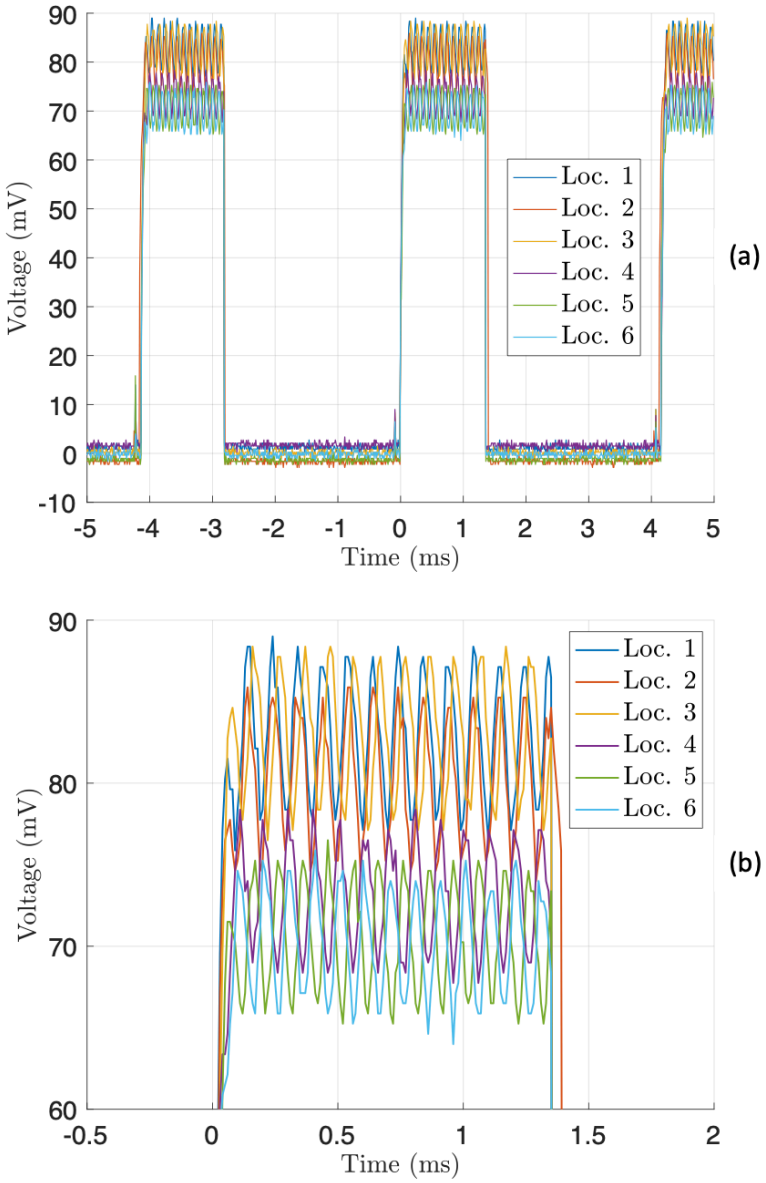


Figure 59: Plot of the measured waveforms in Volts vs Time at photo detector locations 1 through 6. (a) The overall waveforms measured for all 6 locations. The red LED is On for a pulse width of 1.39 ms out of 4.17 ms period. (b) The zoomed-in top sections of the measured signals for all 6 locations. Locations 1 – 3 have uniform illumination relative to each other. Locations 4 – 6 have uniform illumination relative to each other. Locations 1 – 3 have higher amplitude than locations 4 – 6 due to the closer proximity to the source.

Figure 59 shows a plot of the measured waveforms at locations 1 through 6. The overall shape of the waveforms is as expected as the red LED generates an On state pulse width equal to one-

third of the period (1.39 ms pulse width out of 4.17 ms period). If the green and blue LEDs are also used, the gaps in the waveform will be filled. The photo detector measurements show the overall shape of the waveforms is consistent for all six locations. It can be seen that the main difference between the waveforms is the measured amplitude which varies according to the photo detector's proximity to the source. The measured amplitudes for locations 1 – 3 are approximately equal due to uniform illumination. Similarly, the measured amplitudes for locations 4 – 6 are approximately equal due to uniform illumination. The measured waveforms for locations 1 – 3 have higher amplitude compared to the measured waveforms of locations 4 – 6. Figure 59 shows that the overlap of all of the waveforms confirms the transmitted waveform from the DMD does not change at different locations, only the spatial intensity. Thus, the measurements at locations 1 through 6 ensure the DMD has uniform illumination at varying distances from the source. Uniform illumination within a coverage area can be expected with a QKD source that evenly illuminates the DMD.

5.4.2 Constant and Time-Invariant Signal Test

The aim of this experiment is to examine whether the Lightcrafter 4500 can hold the DLP4500 DMD micromirrors in a sufficiently stable state to allow QKD detection. Typically, QKD links use gating windows that span several nanoseconds. The measured waveform of location 5 from Figure 59 is analysed to understand the temporal variations in the emitted signal. Figure 60 shows the top section of the waveform.

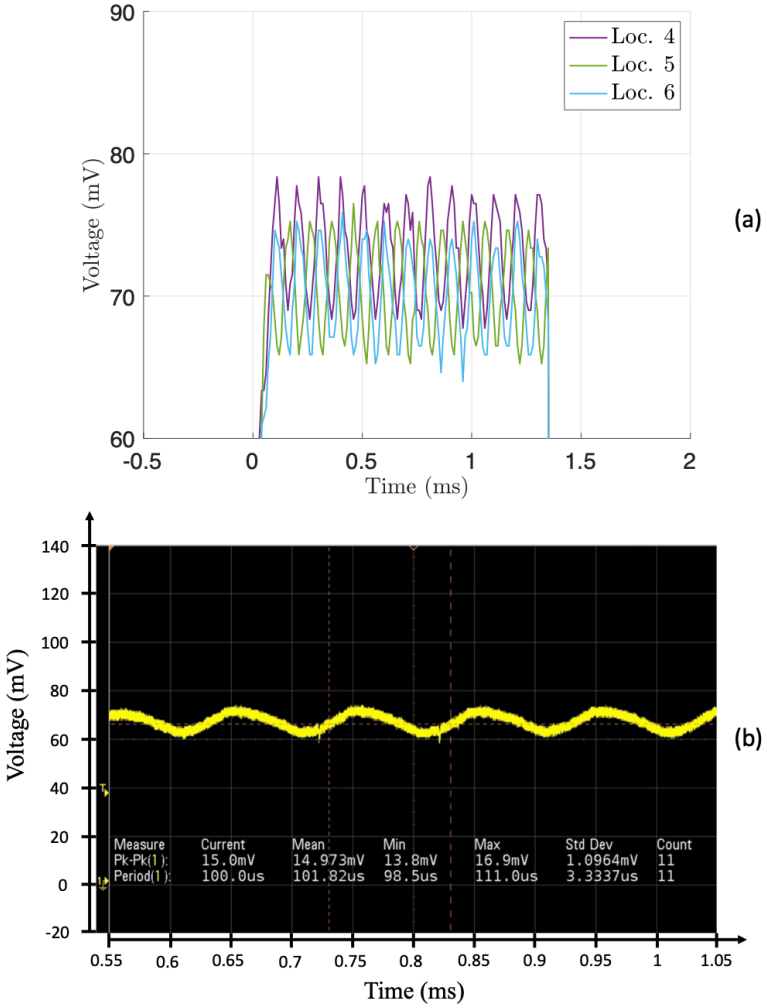


Figure 60: Plot of the top section of the waveform for location 5 in Volts vs Time. (a) The zoomed-in top sections of the measured signals for locations 4 – 6. (b) This is an oscilloscope measurement of the top section of the measured pulse at location 5. The ripple effect is due to the load-reset state of the DMD micromirrors.

The DMD micromirrors in the On state have a waveform that ripples every 100 µs (peak to peak). The cause of the ripple effect is due to the switching state of the micromirrors. The DMD micromirrors are memoryless and receive load-reset commands from the digital controller board. Effectively, the mirrors are controlled every 100 µs to stay in the same state or change states. The pulse width of the On state is 1.39 ms and the 100 µs period is a small portion (7.2%) of the pulse width. This small ripple of the On state suggests that the crest of the 100 µs ripple

can be used to send and receive QKD signals using a gating window at least thirteen times during the On state.

In Figure 60b the waveform of the ripple is sampled every 10 µs by the oscilloscope. The crest of the ripple is relatively flat for 20 µs (±10 µs on either side of the peak). The average peak voltage is 75.2 mV and the average difference in the voltage levels comparing the peak to ±10 µs on either side is 1.8%. This small difference shows the crest of the ripple is relatively flat and suggests the crest could potentially be flatter with resolution smaller than 10 µs. With QKD signals at nanosecond timescales, it is possible for a QKD receiver to use tens of thousands of gating windows within 20 µs around the crest. It could also be possible to relax the gating window constraint to use microsecond timescales instead nanosecond timescales. Therefore, any variation in the DMD micromirrors will not cause a significant effect on the QKD signal. The DMD micromirrors can hold a sufficiently stable state for QKD detection.

5.4.3 Linearity in Pixel Illumination Test

The aim of this experiment is to demonstrate the DMD can modulate a precise number of pixels to illuminate a target area. The experimental apparatus consists of the Lightcrafter 4500 and a Newport 1919-R power meter. The calibrated photodiode sensor on the power meter is 818-SL/DB with a sensor size of Ø11.3 mm. The minimum measurable power is 20 pW and the maximum measurable power is 2 W. The Lightcrafter 4500 is operated in a mode where one DMD micromirror is projected as one pixel of the image on a screen. The red LED is chosen out of the three sources in the Lightcrafter 4500 for this experiment. The Lightcrafter 4500 uses 50% PWM for the output brightness of the red LED. The power is measured for one pixel, then two, then four, then eight. The background illumination is measured for each pixel measurement as a baseline. Table 23 shows the power measurements for the red LED for one

to eight pixels. The projected pixel area was 2.5 mm x 2.5 mm. The sensor size is 16x larger than a single projected pixel.

Table 23: Power measurements for the red LED for one to eight pixels. The signal power is measured for each pixel and the background illumination. The net power of each pixel is calculated from the difference in signal to background power levels. The ratio of the pixels is calculated with reference to the power of one pixel.

N red LED pixel(s) (50% PWM)	P_{Signal} (µW)	$P_{Background}$ (µW)	$P_{N\ Pixel}$ (µW)	$\frac{P_{N\ Pixel}}{P_{1\ Pixel}}$ where N = 1, 2, 4, 8
1	1.013	0.728	0.285	1.0
2	1.930	1.366	0.564	1.979
4	2.489	1.364	1.125	3.947
8	3.620	1.363	2.257	7.919

The pixel signal power ($P_{N\ Pixel}$) is calculated from the difference in each measured signal value (P_{Signal}) from the measured background scatter ($P_{Background}$). The column of $\frac{P_{N\ Pixel}}{P_{1\ Pixel}}$ is the ratio of pixel signal powers of N = 2, 4, and 8 with reference to N = 1. It can be seen in Table 23 that the results in column $\frac{P_{N\ Pixel}}{P_{1\ Pixel}}$ are incremental, linear power levels which correspond to the number of pixels. Hence, the DMD can control a precise number of pixels by linearly scaling them to illuminate an area.

5.5 Analysis of Polarisation Bases Reflected off DMD Micromirrors

The polarisation bases H, V, D, A reflected off the DMD micromirror surface must be maintained as close to the incident polarisation. Figure 61 shows a DMD positioned at an incident angle of 34.5˚ with respect to the optical axis of a QKD transmitter using the BB84 protocol. The purpose of this incident angle is to have the DMD reflect the incident light during the On state through the lens at 45˚. The angles for θ_{ON}, θ_{FLAT}, and θ_{OFF} are calculated using

Eq. (60) – (62). The light reflected to the flat and off states are absorbed by a beam block. The DMD micromirrors are made of aluminium.

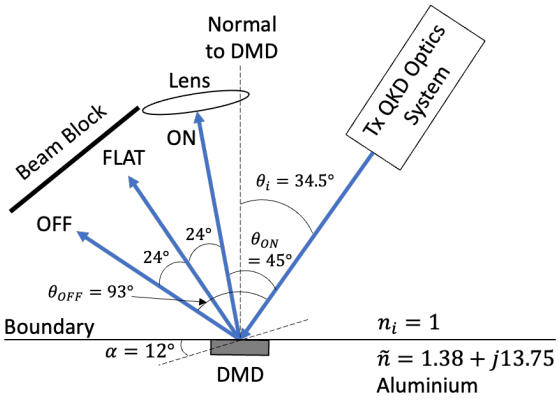


Figure 61: Diagram of the angular position of the DMD and the three states with respect to the QKD transmitter. The refractive index n_i is denoted as free-space. The DMD is made of aluminium with a complex refractive index $\tilde{n}$.

The effect of the DMD surface reflection on the polarisation basis is analysed using Snell's law, the Fresnel equations for reflectance of the 's' and 'p' polarisations, and the complex refractive index ($\tilde{n}$) of aluminium. The equations in this section can be found in [220].

Snell's law is defined as

$$n_i \sin\theta_i = n_t \sin\theta_t \tag{63}$$

where n_i is the medium of the incident electric field, θ_i is the incident angle, n_t is the medium of transmitted electric field, and θ_t is the transmitted angle.

The Fresnel equations for reflection in the 's' and 'p' polarisations of the electric field are defined as

$$r_s = \frac{n_i \cos\theta_i - n_t \cos\theta_t}{n_i \cos\theta_i + n_t \cos\theta_t} \tag{64}$$

$$r_p = \frac{n_t \cos\theta_i - n_i \cos\theta_t}{n_i \cos\theta_t + n_t \cos\theta_i} \tag{65}$$

$$R_s = r_s^2 \tag{66}$$

$$R_p = r_p^2 \tag{67}$$

$$R = \frac{1}{2}\left(R_s + R_p\right) \tag{68}$$

where r_s is the amplitude reflection coefficient of 's' polarisation, r_p is the amplitude reflection coefficient of 'p' polarisation, R_s is the reflectance of the 's' polarisation, R_p is the reflectance of the 'p' polarisation, R is the total reflectance, n_i is the refractive index of the medium for the incident electric field, n_t is the refractive index of the medium for the transmitted electric field, θ_i is the incident angle, and θ_t is the transmitted angle. The reflected power of the 's' and 'p' polarisations of the optical field is the square of the amplitude coefficients of the electric fields. Typically this is shown as the reflectance R_s and R_p at the boundary which is at the aluminium surface of the DMD micromirrors.

In order to simplify the equations and eliminate θ_t, Eq. (63) is rearranged and substituted into Eq. (69). Next, Eq. (69) is substituted into Eq. (70) – (71) with the incident angle $\theta_i = \theta$. θ is the incident angle with respect to the normal of the On state.

$$\cos\theta_t = \sqrt{1 - (\sin\theta_t)^2} = \sqrt{1 - \left(\frac{n_i}{n_t}\sin\theta_i\right)^2} \tag{69}$$

$$R_s = r_s^2 = \left(\frac{n_i\cos\theta - n_t\sqrt{1 - \left(\frac{n_i}{n_t}\sin\theta\right)^2}}{n_i\cos\theta + n_t\sqrt{1 - \left(\frac{n_i}{n_t}\sin\theta\right)^2}}\right)^2 \tag{70}$$

$$R_p = r_p^2 = \left(\frac{n_t\cos\theta - n_i\sqrt{1 - \left(\frac{n_i}{n_t}\sin\theta\right)^2}}{n_i\sqrt{1 - \left(\frac{n_i}{n_t}\sin\theta\right)^2} + n_t\cos\theta}\right)^2 \tag{71}$$

In Figure 61 the DMD surface is made of aluminium. Metal has a complex refractive index

$$\tilde{n} = n_R - jn_I \tag{72}$$

where $\tilde{n}$ is the complex refractive index, n_R is the real refractive index, and n_I is the absorption coefficient. The parameters n_R and n_I are real numbers and wavelength dependent due to the material. The complex refractive index of aluminium [291] at 1371.5 nm is $\tilde{n} = 1.38 + j13.75$.

By substituting $n_i = 1$, $n_t = \tilde{n}$ into Eq. (70) – (71) and assuming $|\tilde{n}|^2 = n_R^2 + n_I^2 \gg 1$, the Fresnel equations for the R_s and R_p coefficients are reduced to

$$R_s = \left(\frac{\cos\theta - \tilde{n}}{\cos\theta + \tilde{n}}\right)^2 = \frac{(n_R - \cos\theta)^2 + n_I^2}{(n_R + \cos\theta)^2 + n_I^2} \tag{73}$$

$$R_p = \left(\frac{\tilde{n}\cos\theta - 1}{1 + \tilde{n}\cos\theta}\right)^2 = \frac{(n_R - \sec\theta)^2 + n_I^2}{(n_R + \sec\theta)^2 + n_I^2} \tag{74}$$

In Figure 61 the On state of the DMD passes through the lens at an angle of 45˚ with respect to the optical axis. Eq. (61) can be rearranged to solve for θ, the incident angle with respect to the normal of the On state. As the mirror is tilted at $\alpha = 12°$ for the On state, $\theta = \frac{1}{2}\theta_{ON} = \theta_i - \alpha = 22.5°$.

Figure 62 shows a plot of the reflectance coefficients R_s and R_p for aluminium at 1371.5 nm. At an incident angle of $\theta = 22.5°$ the reflectance coefficients are $R_s = 0.974$ and $R_p = 0.969$. These coefficients are approximately equal to $R_s = R_p = 0.9717$ at normal incidence. The differences are 0.0023 and 0.0027 respectively

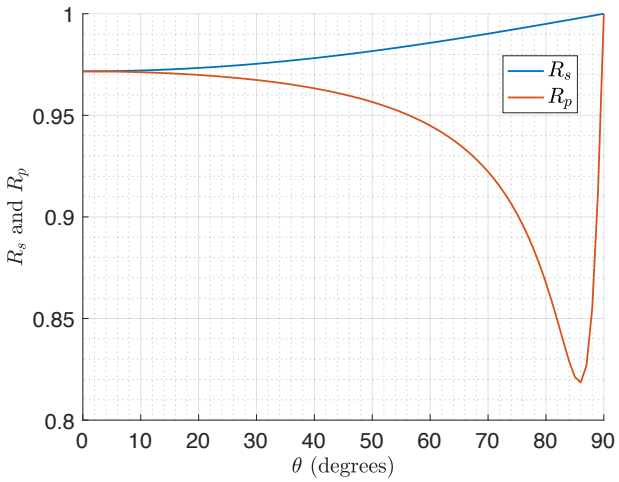


Figure 62. Plot of reflectance coefficients R_s and R_p for aluminium at 1371.5 nm vs the incident angle with respect to the normal of the On state θ in degrees.

Figure 63 shows a plot of the real coefficients of the complex refractive index for r_s and r_p. $r_s = -0.978$ at an incident angle of $\theta = 22.5°$ reflected off the DMD surface. This is approximately equal to $r_s = -0.975$ at normal incidence and the difference is 0.003. $r_p = 0.973$ at an incident angle of $\theta = 22.5°$ reflected off the DMD surface. This is approximately equal to $r_p = 0.975$ at normal incidence and the difference is 0.002.

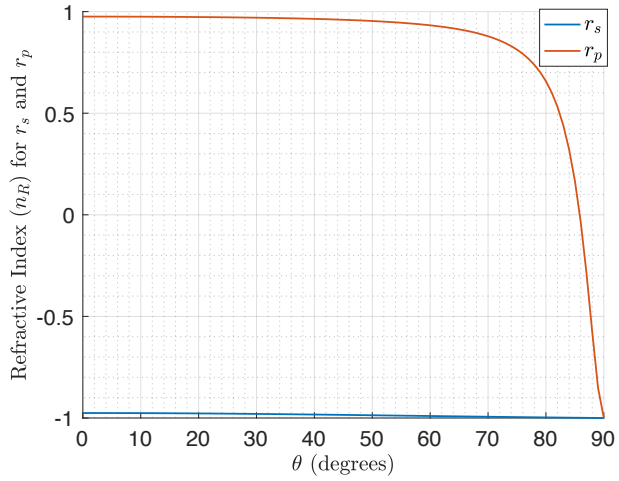


Figure 63. Plot of the real refractive index (n_R) of the amplitude reflection coefficients r_s and r_p vs the incident angle with respect to the normal of the On state θ in degrees.

Figure 64 shows a plot of the phase shifts of the amplitude reflection coefficients r_s and r_p. $r_s = 172.4°$ at an incident angle of $\theta = 22.5°$ reflected off the DMD surface. This is approximately in-phase with $r_s = 171.8°$ at normal incidence and the difference is 0.6˚. $r_p = 8.91^{\circ}$ at an incident angle of $\theta = 22.5°$ reflected off the DMD surface. This is approximately in-phase with $r_p = 8.23^{\circ}$ at normal incidence and the difference is 0.68˚.

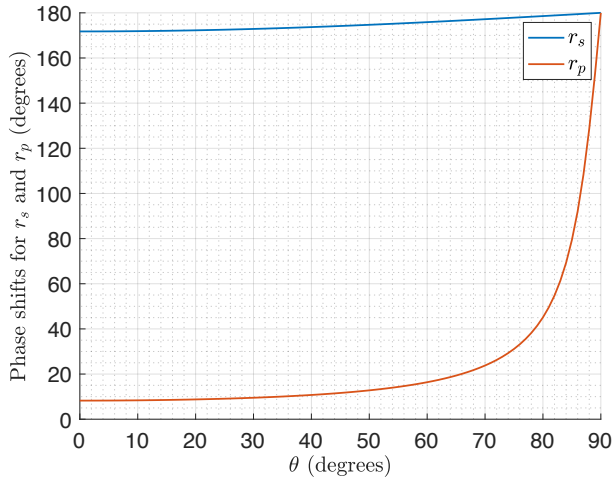


Figure 64: Plot of the phase shifts of amplitude reflection coefficients r_s and r_p vs the incident angle with respect to the normal of the On state θ in degrees.

Figure 62 shows the reflectance coefficients are different at angles larger than normal incidence with respect to the On state. The difference in the reflectance coefficients ($R_s \neq R_p$) implies the amplitude reflection coefficients are different and their phases shift. It can be seen in Figure 64 that the phases are slightly different at the angle of incident at 22.5˚ compared to normal incidence. Therefore, the changes in the relative phases of the amplitude reflection coefficients causes an ellipticity in the reflected polarisation basis. The difference between R_s and R_p is 0.005 at an incident angle of 22.5˚. This causes a slight ellipticity in the reflected polarisation basis and will only affect the Diagonal and Anti-diagonal bases. The slight misalignment to the polarisation bases could increase the QBER at the QKD receiver; however, it can be considered negligible compared to the imperfections in the optical components of the QKD receiver (see

crosstalk matrices in chapter 4 section 4.6.1) and polarisation mismatches Δe of 0.025 which are approximately one order of magnitude larger.

The differences between incident angles 0˚ and 22.5˚ in amplitude and phase shifts of r_s and r_p are minimal. The change in amplitude for r_s is 0.003. The change in amplitude for r_p is 0.002. The change in phase shift for r_s is 0.6˚. The change in phase shift for r_p is 0.68˚. Effectively, the polarisations are linear when reflected off the DMD micromirror surface. Furthermore, the values of R_s and R_p are approximately equal to unity. Thus, the remaining polarisation analysis in this section uses Jones matrices to model the effects of the DMD micromirror surface on the polarisation state of the electric field. Jones matrices in normalised form are

$$H = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \tag{75}$$

$$V = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \tag{76}$$

$$D = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} \tag{77}$$

$$A = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix} \tag{78}$$

Eq. (79) shows the Jones matrix for a mirror at normal incidence [292].

$$J_{Mirror} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \tag{79}$$

Figure 64 shows the phase shifts of the reflected ‘s’ and ‘p’ polarisations are fairly flat and approximately equal to the phase shifts at normal incidence. Therefore, it is assumed the effect of the DMD surface on the reflected polarisation basis can be calculated with a mirror at normal incidence. The polarisations reflected off the DMD surface are

$$H_{reflected} = J_{Mirror} H = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = H \tag{80}$$

$$V_{reflected} = J_{Mirror}V = \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}\begin{bmatrix}0\\ 1\end{bmatrix} = \begin{bmatrix}0\\ -1\end{bmatrix} = e^{j\pi}V \quad (81)$$

$$D_{reflected} = J_{Mirror}D = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}\begin{bmatrix}1\\ 1\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\ -1\end{bmatrix} = A \quad (82)$$

$$A_{reflected} = J_{Mirror}A = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}\begin{bmatrix}1\\ -1\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\ 1\end{bmatrix} = D \quad (83)$$

In Eq. (80) the Horizontal polarisation reflected off the DMD surface remains unaffected. It can be seen in Eq. (81) – (83) that the reflected Vertical polarisation is affected by a π phase shift and reflected Diagonal and Anti-diagonal polarisations are affected by a $\pi/2$ phase shift. A BB84 receiver design can rotate a half wave plate at the D/A channel ports to remove the phase shifts in the reflected Diagonal and Anti-diagonal polarisations.

5.6 Pointing, Acquisition, and Tracking System with DMD and Retroreflector

An indoor free-space QKD link requires a pointing, acquisition, and tracking (PAT) system to maintain line-of-sight (LOS) communications link between a QKD transmitter and a QKD receiver. In a PAT system, a transmitter uses beam steering techniques to point in the general direction of a receiver. Then a transmitter acquires the precise location of a receiver. This is also called localisation. The receiver provides an active or passive signal indicating its location. An example of an active signal is a beacon, which is typically an LED or laser that operates at a different wavelength from the transmitter. Several examples of free-space QKD experiments using beacons have been reported [55, 103, 149]. A passive signal can be provided by a retroreflector, which reflects incident light directly back to the source. Examples of retroreflectors are commonly found on bicycles, helmets, and road traffic signs. In 2018, Rabinovich et al. used a corner cube retroreflector on a drone in a surface-to-drone free-space

QKD link. This experiment used a retroreflector for tracking and also tested the concept of a modulating retroreflector as a quantum source [148].

An experiment was conducted to test a PAT system that consists of the Lightcrafter 4500, a pellicle beam splitter (Thorlabs BP245B3), a retroreflector, and a visible light camera (PhotonFocus MV-D1024-160-CL-8). The Lightcrafter 4500 was used for illumination and beam steering. The retroreflector was used for localisation. The pellicle beam splitter and visible light camera were used for tracking. Figure 65 shows the experimental setup of the PAT system.

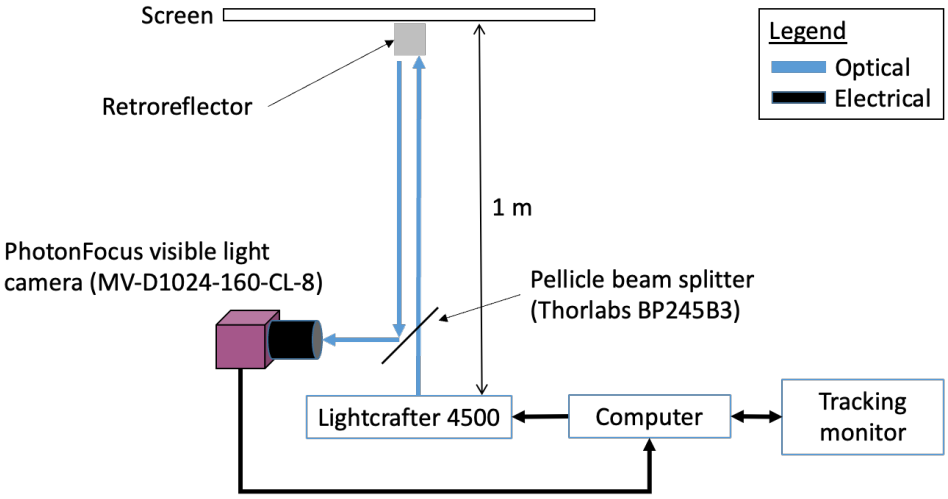


Figure 65: Block diagram of the experimental setup for the PAT system. The distance from the Lightcrafter 4500 to the screen is one metre. The Lightcrafter 4500 is used as an extended monitor display. The pellicle beam splitter is used to ensure there is no chromatic dispersion of the transmitted beam and no ghost reflection on the tracking camera from the retroreflected signal. The pellicle beamsplitter (Thorlabs BP245B3) is suitable for visible wavelengths [293].

The PAT system was controlled via a Matlab script. The Matlab script instructed the Lightcrafter 4500 to illuminate a screen with white light, which was created from the red, green, and blue LEDs inside the Lightcrafter 4500. The Matlab script then isolated the retroreflected light on a tracking monitor and estimated the coordinates of the centroid for the retroreflected

light. Finally, the Matlab script instructed the Lightcrafter 4500 to send a blue spot to the centroid coordinates. The blue LED was chosen out of the three sources to illuminate a spot because the colour had the highest contrast with respect to the retroreflector surface. The size of the blue spot was chosen to fit within the retroreflector area. Figure 66 shows a picture of the retroreflector illuminated by the Lightcrafter 4500.

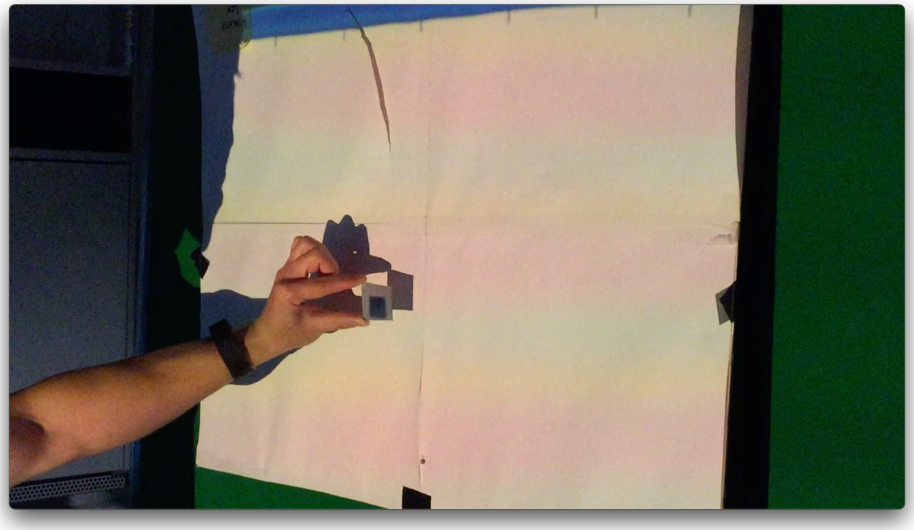


Figure 66: Picture of a retroreflector illuminated by the Lightcrafter 4500. The blue spot indicated the estimated centroid coordinates of the retroreflector using the PAT system. The blue LED was chosen out of the three sources in the Lightcrafter 4500 to illuminate a spot that has the highest contrast with respect to the retroreflector surface.

5.7 Plan to Incorporate a DMD at the QKD Transmitter

The previous sections have shown the feasibility of the DMD (DLP4500) as part of a quantum transmitter and PAT system. This section details a plan to incorporate a NIR coated version of the DMD (DLP4500NIR) into the QKD transmitter from section 4.3.1 without the Ø12 mm iris at the output of the spatial filter. The DLP4500NIR [294] can reflect the QKD wavelength at 1371.5 nm. Figure 67 shows a block diagram of the planned experimental QKD system with the DMD incorporated into the QKD transmitter.

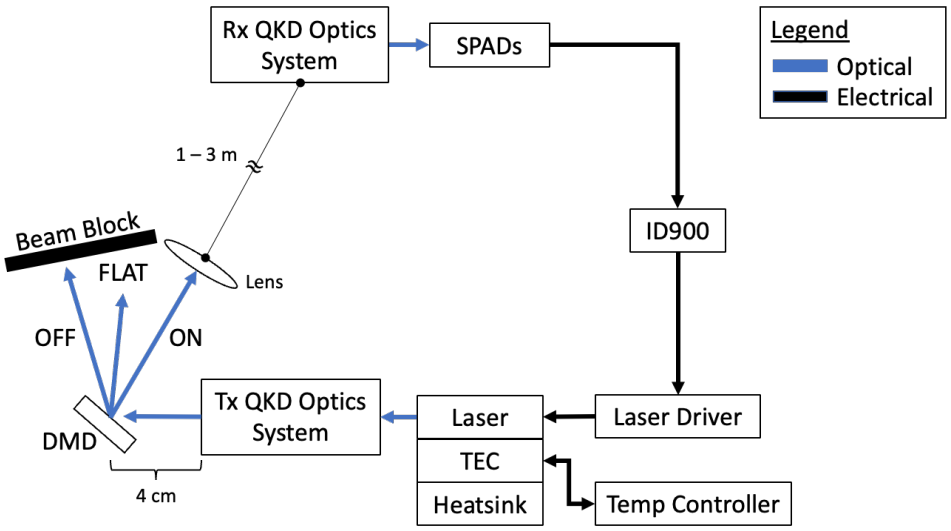


Figure 67: Block diagram of the planned experimental QKD system with the DMD incorporated into the QKD transmitter.

In Figure 67, the DMD is located at 4 cm away from the Tx QKD Optics System. The DMD is positioned at a 34.5˚ incident angle with respect to the optical axis of the Tx QKD Optics System. The output of the Tx QKD Optics System is the spatial filter. The output of the spatial filter has a beam diameter ~12.78 mm (section 4.3.1.3) which is larger than the diagonal of the DMD (11.62 mm). The Gaussian beam profile is incident on the DMD and overfills the entire area of the DMD. As a result, the centre pixels will have more intensity than the edge pixels and the edge pixels have near $\frac{1}{e^2}$ levels of intensity. The Rx QKD Optics System is based on the QKD receiver design in Chapter 4 Figure 43. This receiver design must rotate the half wave plate at the D/A channel ports to remove the phase shifts in the reflected Diagonal and Anti-diagonal polarisations. Consequently, the reflections off the DMD surface are not an issue for the planned experimental QKD system with the DMD at the QKD transmitter.

There is a design constraint for the lens in the QKD transmitter apparatus. The lens used to image the DMD pixels is Thorlabs LA1102-C which is a Ø30 mm lens with effective focal length 5 cm. This lens is chosen due to the space constraints for the incident light on the DMD and the three states of the DMD. The minimum distance for the reflection off the Flat state to hit the beam block and not interfere with the On state of the DMD is 5 cm. The distance between

the DMD and the lens should be kept to a minimum in order to maximise the magnification of the pixels. The magnification of a lens is

$$M = \frac{q}{p} \tag{84}$$

where q is the distance from the image plane to the lens and p is the distance from the object plane to the lens. The DMD is positioned at $p = 5$ cm away from the lens. At distances $q = 100$ cm and $q = 300$ cm away from the lens, the magnification along one dimension of the pixel (i.e. the length) is $M = 20$ and $M = 60$, respectively. At 300 cm away, the total coverage area is equivalent to 3.5x A4 size sheets of paper.

Currently the system is limited by the spatial resolution of the DMD with a 912 x 1140 micromirror array. A higher resolution DMD can potentially provide more precise spot beams for coverage. With regards to resolution, an example of a 4K Ultra High Definition resolution (3840 x 2160) DMD is Texas Instruments DLP471TP [295]. The DLP471TP has a diagonal of 0.47 inches (1.2 cm) with a 1920 x 1080 micromirror array. The 4K image is created by pixel shifting two 1920 x 1080 images slightly next to each other so the images overlap. The technology responsible for pixel shifting is eXpanded Pixel Resolution (XPR) and DMD's with this technology can operate up to 240 Hz. This is at least twice the frame rate of the DMD used in this thesis (DLP4500). The physical size of the DLP471TP is similar to the DLP4500; however the micromirror array is 2x larger than the DLP4500 micromirror array. The 4K resolution DMD offers 8x more precision for spot beams with similar coverage area (3.5x A4 size sheets of paper). Larger DMDs can potentially provide larger magnified areas of coverage. With regards to size, the largest DMD sold by Texas Instruments is DLP9500 [296]. The DLP9500 has a diagonal of 0.95 inches (2.4 cm) with High Definition resolution (1920 x 1080). The total coverage area is equivalent to 49x A4 size sheets of paper (14x the DLP4500 coverage area) and provides 2x more precision in spot beams. Both examples of DMD increase the spatial

resolution of the system and allows for individual mirrors to be controlled for different areas of the room, potentially without the need for beam steering.

The DMD can modulate pixels to create a beam spot that will fit within the collection area of the QKD receiver. In Figure 67, it is assumed the Rx QKD Optics System is the same QKD receiver as in section 4.4.4. The Rx would require a maximum beam spot size of Ø6 mm circular diameter due to the collimator (Thorlabs F280FC-C). The number of pixels to be magnified is based on the Eq. (85) – (86)

$$\mathrm{A}_{Rx,spot} = M^2 \mathrm{A}_{DMD,spot} \tag{85}$$

$$N_{pixel} = \frac{\mathrm{A}_{DMD,spot}}{\mathrm{A}_{pixel}} = \frac{\mathrm{A}_{Rx,spot}}{M^2 \mathrm{A}_{pixel}} \tag{86}$$

where $\mathrm{A}_{DMD,spot}$ is the area of the Gaussian beam spot on the DMD, M is the magnification, $\mathrm{A}_{Rx,spot}$ is the area of the beam spot at the QKD receiver, A_{pixel} is the area of one DMD pixel, and N_{pixel} is the number of pixels used by the DMD to be magnified to fill the receiver area. For example, the length and width of the DMD mirrors is 7.637 µm each; hence the area of one DMD pixel is 58.3×10^{-12} m^2. At $q = 100$ cm and $M = 20$, the number of pixels the DMD would need to use to fill a Ø6 mm beam spot at the QKD receiver is

$$N_{pixel} = \frac{\mathrm{A}_{Rx,spot}}{M^2 \mathrm{A}_{pixel}} = \frac{\frac{\pi}{4}(0.006)^2}{(20^2)(58.3 \times 10^{-12})} = 1{,}212 \tag{87}$$

Table 24 shows the minimum number of pixels necessary for the DMD to create a beam spot at link distances of 100 cm and 300 cm. The beam spot sizes are Ø3 mm and Ø6 mm circular diameters at the QKD receiver.

Table 24: Minimum number of pixels for the DMD to create two beam spot sizes at the QKD receiver for 100 cm and 300 cm link distances.

	$q = 100$ cm $M = 20$	$q = 300$ cm $M = 60$
Area of beam spot at QKD Rx $A_{Rx,spot}$	**Number of DMD pixels N_{pixel}**	**Number of DMD pixels N_{pixel}**
$\frac{\pi}{4}(Ø3\ mm)^2$	303	34
$\frac{\pi}{4}(Ø6\ mm)^2$	1,212	135

5.8 Plan to Incorporate a DMD at the QKD Transmitter with a Pointing, Acquisition, and Tracking System

A pointing, acquisition, and tracking (PAT) system is necessary for an indoor QKD link. A QKD transmitter can illuminate a desired coverage area with white light to find a retroreflector which may be in a QKD receiver. A similar function can be accomplished with the DMD as an illumination device to show where a QKD signal is available and for tracking. This section details a plan to incorporate the PAT system from section 5.6 with the planned QKD system from section 5.7.

5.8.1 System Architecture

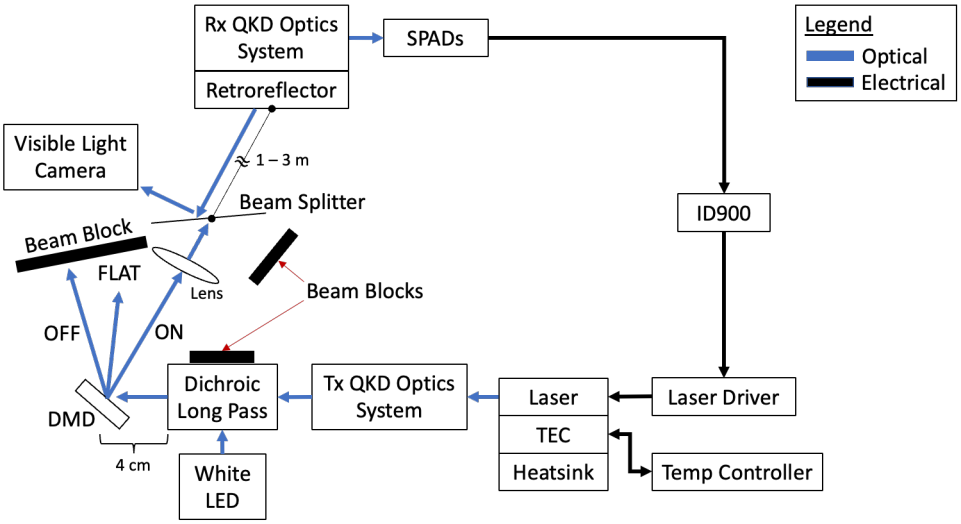


Figure 68: Block diagram of the planned system architecture with the PAT system (section 5.6) incorporated into the QKD system (section 5.7). The quantum channel is denoted as the path from the Tx QKD Optics System through the dichroic long pass filter, reflected off the DMD, and to the Rx QKD Optics System. The classical channel is denoted as the path from the white LED source reflected off the dichroic long pass filter, reflected off the DMD, reflected back from the retroreflector to the beam splitter and onto the visible light camera. The LED source has wavelengths between 380-780 nm and is used for illumination and tracking purposes only, not for visible light communications. The visible wavelengths do not interfere with the QKD operational wavelength at 1371.5 nm.

Figure 68 shows a block diagram of the planned experimental system architecture with the PAT system from section 5.6 incorporated into the QKD system from section 5.7. The diagram shows the planned PAT system consists of a white LED, dichroic long pass filter, retroreflector, beam splitter, and visible light camera. It is assumed that within the coverage area of the DMD, the QKD receiver is manually aligned with the QKD transmitter. This ensures the retroreflector is tracked by the visible light camera. This classical channel is used for illumination and tracking purposes only and a white LED is considered for the PAT system. An example of a white LED is SORAA SM16C-CC1-10D-927-03-S3 [297]. This LED can be used because of its brightness and spectrum. The excitation wavelength of the SORAA LED is near 400 nm and

the yellow phosphor has an emission peak near 600 nm. This LED has a wavelength range of 380 – 780 nm. This spectrum is far away from the QKD wavelength of operation at 1371.5 nm that was used in chapter 4. Hence, the SORAA LED can be used for the classical channel to ensure the illumination does not interfere with the quantum channel. The QKD channel uses fibre lasers at 1371.5 nm to send the single photons. Similar to the BB84 experiment in chapter 4 section 4.5, the ID900 Time Controller is the central node between the QKD transmitter and receiver in this experimental system architecture.

In operation, the DMD would be located at 4 cm away from the dichroic long pass filter. The dichroic long pass filter (i.e. Edmund Optics 87-046) would be used to align the QKD signal from the output of the spatial filter with the white LED (i.e. SORAA SM16C-CC1-10D-927-03-S3). The two beams would be co-linear for the DMD. The PAT method would use the white light emitted from the SORAA lamp to illuminate a retroreflector at the receiver for pointing and acquisition. The retroreflected light would reflect off a beam splitter and into the visible light camera for tracking. The beam splitter must be at a 45º angle of incidence (AOI) to allow the white light to transmit through and the retroreflected signal to reflect back into the visible light camera. The camera would take an image of the retroreflected signal, and the Matlab script would estimate the centroid coordinates of the image. Then, the Matlab script would instruct the DMD to illuminate the receiver with a beam spot the same size as the retroreflector at the estimated centroid coordinates. The SORAA lamp is always on to help illuminate the beam spot at the receiver. It is assumed the QKD receiver is nomadic. Therefore, the Matlab script would continue to instruct the DMD to illuminate and track the retroreflector in a feedback loop until the estimated centroid coordinates are stable. That is, the QKD receiver is stationary and the difference in the previous and current estimated centroid coordinates is approximately zero. Once the QKD receiver is stationary, the Matlab script would instruct the DMD to create a beam spot with a similar number of pixels as shown in Table 24 for 100 cm at the estimated

centroid coordinate. Afterwards, the ID900 would send NIM pulses to the QKD transmitter and the DMD would direct the single photons to the QKD receiver. This process would be repeated for up to 300 cm link distance.

5.8.2 Choice of Beam Splitter

In Figure 68 it is necessary to consider an appropriate beam splitter for the QKD signal and PAT system. In the PAT system test in section 5.6, a Thorlabs BP245B3 pellicle beam splitter is used with the Lightcrafter 4500. The test shows there is enough transmission of white light to illuminate a screen and enough reflection off the retroreflector into the tracking camera. The Matlab script is able to estimate a centroid coordinate of the retroreflected image and instruct the Lightcrafter 4500 to send a spot for tracking the retroreflector.

However, the Thorlabs BP245B3 pellicle beam splitter makes a significant difference in transmittance levels for 'p' and 's' polarisation at near infrared wavelengths. This pellicle beam splitter has a transmittance of 63% for 'p' polarisation and 25% for 's' polarisation at 1371.5 nm. The transmittance levels affect the BB84 signals by changing the amplitude and angle of each polarisation basis. As a result, the BB84 protocol using this pellicle beam splitter will not work. It is necessary to minimise the difference in transmittance of 'p' and 's' polarisation.

A potential solution is to choose a plate beam splitter (i.e. Thorlabs BSW18) that has more even distribution of 'p' and 's' polarisations. The Thorlabs BSW18 is a 50:50 plate beam splitter that has approximately equal transmittance and reflectance at 1371.5 nm (53% for 'p' polarisation and 50% for 's' polarisation). The transmittance and reflectance of visible wavelengths are similar to the Thorlabs BP245B3 pellicle beam splitter. There is an anti-reflection coating that is applied to the back surface of the lens to eliminate ghost reflections.

5.9 Discussions and Observations

Indoor free-space QKD links can benefit from beam steering devices such as a DMD. Initial experimental results with the Texas Instruments Lightcrafter 4500 evaluation board have shown the DMD (DLP4500) is feasible as a quantum transmitter. For quantum applications, the DMD can send a QKD signal that is uniform anywhere within the coverage area. The DMD can hold its micromirrors in the On state much longer than typical QKD operations. The state of the micromirrors is sufficiently stable which ensures little variation in the QKD signal sent to a beam steered location. Also, the DMD can modulate a precise number of pixels to illuminate a target area. There are two advantages: 1) the DMD can illuminate a coverage area to show where a QKD signal can be found and 2) the DMD can send single photons using as few mirrors as possible. This helps confine the transmitted beam to the aperture of the QKD receiver.

Due to the angle of incidence between the DMD and the QKD transmitter, the DMD aluminium surface causes a slight ellipticity to the polarisation basis. Mainly the Diagonal and Anti-diagonal polarisations are affected. The misalignment due to the ellipticity is minimal and can be considered negligible when compared to the imperfect optical components in the QKD receiver. In the experimental plans, the QKD receiver design is based on the QKD receiver from section 4.4.4. This QKD receiver can rotate the half wave plate to remove the added phase shift for the D/A polarisations reflected off the DMD.

An initial experiment was done showing a coarse method for a PAT system using a DMD. However, more work is needed to resolve the number of pixels for a beam spot. The next steps in implementing a PAT system to align the transmitter and receiver using the DMD are outlined in future work.

5.10 Summary

An indoor free-space QKD link requires beam steering to direct light from a QKD transmitter to a QKD receiver. This can be achieved with a tracking system that can be integrated into the transmitter in order to direct the QKD signal to a receiver on a desk within a room. The DMD is a commercial, practical, and cost-effective beam steering device. Initial experimental results with a Lightcrafter 4500 characterised the DMD as suitable for quantum applications and beam steering at the QKD transmitter. The DMD satisfied four requirements for a QKD transmitter: 1) the DMD had uniform illumination within a desired coverage area, 2) the DMD held the micromirrors in a stable state for a sufficient amount of time for QKD detection, 3) the DMD controlled a precise number of pixels to illuminate a target area and 4) maintained the same precise incident polarisation that is reflected off the DMD surface for polarisation-based QKD protocols. The DMD can modulate groups of pixels to enable a pointing, acquisition, and tracking (PAT) system. A PAT system uses beam steering techniques to point the transmitter in the general direction of a receiver. Then a transmitter acquires the precise location of a receiver. The receiver provides an active or passive signal which indicates its location. Lastly, the PAT system tracks the location of the receiver. As part of the PAT system, the DMD can be used to project a total coverage area equivalent to 3.5x A4 size sheets of paper at 3 metres distance. Two plans were discussed about incorporating the DMD into the QKD transmitter and with the PAT system using a retroreflector, beam splitter, and visible light camera.

Chapter 6 Conclusions and Future Work

In this work, we developed a short-range free-space QKD link that is robust to sunlight. We addressed one of the key challenges with indoor free-space QKD links which is to mitigate interference and induced noise from sunlight at the QKD receiver. Sunlight is the main cause for noise in free-space QKD links; hence dark environments are typically used. The choice of wavelength is the key to all QKD systems. Wavelength regions where there is minimal photon counts from sunlight such as atmospheric absorption bands are potential novel regions to explore for indoor free-space QKD.

In Chapter 2, an indoor BB84 QKD link was modelled and simulated with two sources of ambient light: LED lighting and sunlight. The QKD receiver parameters such as a short gating window, narrowband wavelength filtering, and narrow spatial filtering were used to limit the amount of ambient light at the receiver in order to facilitate a QKD link. The QKD link was simulated for two operating wavelengths: 658 and 761 nm. The preliminary modelling showed that operating a QKD link at 658 nm worked under LED lighting; however, 658 nm did not work in sunlight unless a gating window was used with a single mode fibre at the QKD receiver. The wavelength of 761 nm was chosen because it had the lowest photon counts in the visible spectrum. This is due to the Oxygen A absorption band. The preliminary modelling showed that it was feasible to operate a QKD link within this band in sunlight. However, the narrow nature of this band required a narrowband spectral filter (≤ 2 nm). This would limit the field of view of the QKD receiver and such a filter was typically expensive. Hence, it is not a practical wavelength to use. Atmospheric absorption bands for sunlight are good indicators of regions for further investigation.

In Chapter 3, an investigation into the water and carbon dioxide absorption band between 1351 – 1414 nm was undertaken. The photon counts from 1351 – 1414 nm, especially at 1370 nm,

are much lower than that of 761 nm. The water and carbon dioxide absorption band is a flat region which is suitable for wider field of view links and cheaper, wider bandwidth filters. Typically, QKD links require very narrow filter bandwidths and narrow FOV to reduce the sunlight impairments, however the reduced level of sunlight in this band offered promise of more practical QKD links.

A series of experimental measurements using a calibrated Ocean Insight NIR Flame spectrometer and ID Quantique idQube SPAD module showed that a BB84 link should operate at 1370 nm because the sunlight in this region had minimal effect on a QKD receiver. The QKD receiver consisted of a 10 nm passband filter centred at 1370 nm, collimator with single mode fibre, and an idQube SPAD module. A QKD link model was simulated using the experimental measurements from the SPAD module. This simulation showed that a QKD link can operate in direct sunlight at 100k lx with a QBER below 4% and potentially tolerate a 14 dB link loss with a gating window for 1,750 CPS at each SPAD module. Also, for higher sunlight levels and noise counts greater than 100k lx, a QKD link performance with lower link losses can be tolerated. Therefore, sunlight had minimal effect on the QKD receiver around 1370 nm. Furthermore, the water and carbon dioxide absorption band from 1351 – 1414 nm has a potential use in short range links in the presence of sunlight.

The potential benefit of using wavelengths from 1351 – 1414 nm is the close proximity to telecommunications wavelengths. These wavelengths in the E-band can be used in fibre networks using CWDM where each wavelength can be recovered through filtering. Moreover, fibre-only architectures can evolve to fibre-wireless-fibre architectures such that central network offices connect to their satellite offices via fibre and use indoor optical wireless communications for their end-users.

In Chapter 4, an indoor BB84 QKD link was simulated and experimentally demonstrated with a halogen lamp as an analogue to outdoor direct sunlight at 100k lx between 1351 – 1414 nm. The halogen lamp was a suitable substitute for sunlight in the region of interest due to its spectral flatness across the entire bandwidth of the spectrometer. The measured halogen lamp spectrum at 800 lx was equivalent to the outdoor spectral measurement of direct sunlight at 100k lx between 1351 – 1414 nm. The halogen lamp induced 800 CPS at the SPAD module. The indoor BB84 QKD link model was simulated at 1370 nm for a mean photon number μ = 0.1 and two repetition rates: 10 MHz and 41.67 MHz. The results of the simulations showed the QKD links were feasible for QBER $\leq$ 4% and up to 14 dB link loss with a gating window for both 10 MHz and 41.67 MHz repetition rates.

A free-space QKD link using the BB84 protocol in the presence of ambient light was demonstrated. The experiment was a bench top demonstration. The centre wavelength of the QKD system was 1371.5 nm. The link distance was 23 cm. The QKD system was indistinguishable temporally, spectrally, and spatially to guard against side channel attacks from Eve. The pulse shapes were temporally indistinguishable due to the mutual information $I(W:E) \propto 10^{-3}$ bit/pulse. The minimal difference in the pulse shapes ensured all of the lasers operated at the same mean photon number. The laser linewidths were spectrally indistinguishable due to the mutual information $I(\wedge:E) \propto 10^{-4}$ bit/pulse. Spatial filtering was used to remove the fringe noise (outer diffraction rings) of the Gaussian beams and only allowed the central Gaussian spot to pass through.

Two sets of experiments for repetition rates 10 MHz and 41.67 MHz were performed to show repeatability and reproducibility of the results under ambient light. The ambient light used for the QKD link consisted of illumination from LED ceiling lighting and a halogen lamp. The halogen lamp used to simulate the solar spectrum at 100k lx in the water and carbon dioxide

absorption band from 1351 – 1414 nm. The QKD experiments were performed for 30 minutes and 60 minutes under different intervals of ambient light. In the '30 minute' experiments, the QKD system was under complete darkness for 10 minutes, LED ceiling lighting for 10 minutes, and direct illumination from the halogen lamp for 10 minutes. In the '60 minute' experiments, the QKD system was under complete darkness for 10 minutes, LED ceiling lighting for 10 minutes, and direct illumination from the halogen lamp for 40 minutes.

The QKD system performed well under LED lighting and the results were similar to the system under complete darkness. Overall, the QKD system performed well under conditions that resembled outdoor direct sunlight. The QKD system at 1371.5 nm worked under the halogen lamp with an average QBER of 6.5% for at least 40 minutes. Therefore, this result shows the QKD performance can extend to outdoor applications for short range links and indoor environments illuminated by sunlight. The QKD system at 1371.5 nm is robust to sunlight and to the author's knowledge, the first of its kind.

In Chapter 5, a series of experiments with the Texas Instruments Lightcrafter 4500 showed a digital micromirror device (DMD) is feasible for beam steering and quantum applications at the QKD transmitter. The effect of the DMD micromirror surface on the polarisation basis from the QKD transmitter was analysed. Two plans to incorporate the DMD into the QKD transmitter and the overall QKD system were discussed.

The DMD satisfied four requirements for a QKD transmitter:

1) Uniformly illuminate within a coverage area (assuming the QKD source evenly illuminates the DMD).
2) Sufficiently hold the micromirrors in a stable state and a sufficient amount of time for QKD detection (i.e. nanoseconds).

3) Control a precise number of pixels to illuminate a target area.
4) Maintain the same polarisation of the incident beam when reflected off the DMD micromirror surface for polarisation-based QKD protocols.

The advantages of using the DMD at the QKD transmitter are:

1) Illuminate a coverage area to show where a QKD signal can be found.
2) Send single photons using as few mirrors as possible. This helps confine the transmitted beam to the aperture of the QKD receiver.

The DMD aluminium surface causes a slight ellipticity to the polarisation basis. However, this ellipticity is negligible. Effectively, the polarisations that reflect off the DMD are linear with the Diagonal and Anti-diagonal polarisations primarily affected by a $\frac{\pi}{2}$ phase shift. Hence, a BB84 QKD receiver should rotate a half wave plate at the D/A channels to remove the added phase shift for the D/A polarisations reflected off the DMD. The next sections detail the system improvements and future work of this thesis in chronological order with time estimates.

6.1 System Improvements

6.1.1 Degree of Polarisation Experiment (1 week)

The degree of polarisation experiment should consist of the four lasers at the QKD transmitter, a linear polariser, and a low-noise SPAD module such as idQube. The linear polariser should be placed between the spatial filter and the SPAD module. The linear polariser should be rotated by hand to measure the maximum and minimum photon counts for each laser. This experiment is similar to the polarisation angle calibration experiment (chapter 4 section 4.4.1) except the SPAD module replaces the power meter. The SPAD module has a sufficient dynamic range to measure how polarised the qubit states are after the spatial filter.

6.1.2 Visible Light Communications (1 month)

A visible light monochromatic LED or laser source can be substituted into the PAT system and used as a high speed data communications link. The SORAA LED lamp can be substituted with a visible light source that can be modulated. After the dichroic long pass filter, the output beams of the visible light source and QKD transmitter will be co-aligned. This combines free-space optical communications and QKD within the same setup.

6.1.3 Transmitter and Receiver Time Synchronisation for Gating (3 months)

The ID900 controls the timing between the QKD transmitter output pulses and the received timestamps of the qubit states. A form of time synchronisation (i.e. clock pulses) over a wireless public channel should be implemented between the transmitter and receiver. This removes the ID900 connection to the QKD transmitter and makes a more practical implementation of the QKD system. The receiver should use a gating window of 6 ns which is equal to the pulse width of the transmitted pulses.

6.1.4 DMD Tracking System (3 months)

The design of the retroreflector should be a disc that fits around the aperture of the QKD receiver. The next step would be to test the efficiency of the retroreflector design by using the PAT system. The aim of the test is to check whether the retroreflector disc can sufficiently retroreflect the localisation signal back to the tracking camera. A power meter could be used to measure the power distribution of the beam spot at the retroreflector. If the retroreflector concept does not work, a beacon can be used at the receiver. A beacon is a source used to illuminate the location of the receiver back to the camera at the transmitter. The beacon will

use a different wavelength than the transmitter and this design will not require a white LED at the transmitter. Finally, the loop bandwidth of the tracking system should be addressed.

6.1.5 Asynchronous Trigger (3 months)

The DMD has three states of operation: On, Off, and Flat. Flat is the default state when the DMD does not have a voltage applied to it and the mirrors are parked at 0˚ which is parallel to the backplane. The On and Off states pivot to +12˚ and -12˚ with respect to the normal axis to the backplane when a voltage is applied to the DMD. As a result, the back plane of the DMD is exposed when the mirrors pivot to either state. The incoming light that is incident on the DMD is scattered on the backplane of the DMD from all of the gaps between the On and Off state mirrors also known as background scatter. By incorporating the DMD into the transmitter design in Figure 67, it is clear that the DMD would always have to 'throw' the Off state mirrors over to a beam block and 'throw' the On state mirrors toward the lens. In the DLP technology, the contrast ratio is the amount of light flux received from the On state over the background scatter. This can produce some of the deepest colours and mitigate the image from appearing washed out by the input source or ambient light [298]. In a free-space QKD system, the contrast ratio can be used to distinguish the received signal from the background scatter and hence trigger, for example a precursor signal, when a QKD pulse is sent and activates a gating window for the expected arrival of the photon at the receiver. Free-space QKD links that used a precursor signal for timing at the receiver have been reported [109, 112-114].

In operation the QKD receiver would use the illumination of the source as a threshold for synchronisation in the QKD link. Illumination of the source could be a form of asynchronous timing where the transmitter would use a precursor signal to trigger the detection timing window at the receiver. Afterwards, the transmitter would send the QKD signal. The precursor signal has higher power than the QKD signal. Prior to the arrival of the precursor signal, the

receiver would monitor the photon counts from ambient light. After the receiver detects the precursor signal, the receiver would compare the photon counts received from the precursor signal to those from the ambient light. If the difference in photon counts exceeds a signal to noise ratio (SNR) of 30 dB, then the receiver would initiate its detection gating window to receive the QKD signal. As a result, the receiver would be triggered asynchronously to detect single photons for the key. Alice and Bob would share less information over the public channel such as time synchronisation and clock pulses.

6.2 Future Work

6.2.1 Longer Link Distances (1 month)

There is a need to create longer distance links. The QKD link experiment in chapter 4 was demonstrated for a 23 cm link distance. However, the distance needs to be extended to 3 or 4 metres (i.e. the full height of a typical office room environment) to truly demonstrate the practicality of this QKD system for indoor optical wireless communication links. The link distance could be extended with the receiver on another optical table 3 metres away to simulate the full scale room setup. The optical table should have wheels to simulate nomadic movement of the receiver and to help test the PAT system.

6.2.2 Transmitter and Receiver Alignment (3 months)

The transmitter and receiver have to align reference frames for the BB84 protocol and other polarisation-based protocols (except for the Reference Frame Independent QKD protocol). In the QKD link experiments for this thesis, the polarisers are aligned at the transmitter and receiver because the setups are on the same optical table. The optical table fixes the same reference frame for the transmitter and receiver. If either setup is on another optical table or platform that is rotated slightly, the reference frames need to be realigned. A half wave plate

can be installed in front of the non-polarising beam splitter in the receiver to rotate the received polarisations and align with the receiver reference frame. The receiver must communicate with the transmitter over the public channel about its location, orientation, and the amount of rotation between the receiver and the transmitter. This could be possible with GPS coordinates, azimuth and elevation, and a reference to compass North.

6.2.3 Smaller Transmitter Form-Factor (3 months)

The size of the transmitter can be reduced with smaller components. Also, the laser driver, controller boards for the laser driver, heatsinks, and temperature controller boards can be consolidated into a more compact form with the optics. One possible design could have the system electronics and optics stacked in a box where the electronics are on the bottom with the optics on top.

6.2.4 Further Investigation into 1351 – 1414 nm Spectral Region (1 month)

Further investigation into the 1351 – 1414 nm region is necessary to characterise this region more accurately for QKD. It is clear that the water and carbon dioxide absorption band (1351 – 1414 nm) has substantially lower spectral content from the ultraviolet to the near infrared spectrum. The measured spectrum using the calibrated NIR Flame spectrometer with Ø600 µm fibre and cosine corrector (Ocean Insight FLAME-NIR-INTSMA25) and the ASTM spectrum at the same lux level are significantly different. The ASTM standard is flat and nearly zero across the entire band while the measured spectrum is approximately 8x the ASTM spectrum within the same band. Further investigation into the difference is needed.

6.2.5 RFI QKD Protocol (6 months)

The next protocol to implement in this system is the Reference Frame Independent QKD (RFI-QKD) protocol. The RFI-QKD protocol is the leading candidate for future protocol implementation as it is more robust than the classical BB84 protocol in a practical room environment. The RFI-QKD protocol requires six polarisations at the transmitter and receiver. The RFI-QKD protocol was implemented in a handheld free-space QKD experiment in [55]. At present, the BB84 protocol requires the transmitter and receiver be on the same reference plane for Alice and Bob to compare the same polarisation basis. In a room environment the receiver can be anywhere in the room, and their reference frame with respect to the transmitter will need to be heralded in order for the transmitter to rotate and align itself to the receiver. This added complexity requires additional engineering to the pointing, acquisition, and tracking (PAT) system. However, the RFI protocol relaxes the reference frame requirement which is especially useful with the DMD as a user can be anywhere in the room and not have to align their reference frame with the transmitter.

References

[1] A. Banafa, "Three major challenges facing IoT," *IEEE IoT Newsletter,* 2017.

[2] N. Aleisa and K. Renaud, "Privacy of the Internet of Things: A Systematic Literature Review (Extended Discussion)," *arXiv preprint,* 2016, doi: 10.48550/arXiv.1611.03340.

[3] M. Bartock, J. Cichonski, and J. Franklin, "LTE Security–How Good Is It?," *NIST, Gaithersburg, MD, USA, Tech. Rep,* vol. 3, 2015. [Online]. Available: https://csrc.nist.gov/CSRC/media/Presentations/LTE-Security-How-Good-is-it/images-media/day2_research_200-250.pdf.

[4] E. Griffith, "How to Hack Wi-Fi Passwords," *PCMag UK,* 2024. [Online]. Available: https://uk.pcmag.com/networking/40259/how-to-hack-wi-fi-passwords.

[5] Think broadband, "Fibre Broadband (FTTC/FTTH) Guide," [Online] 2017. [Online]. Available: https://www.thinkbroadband.com/guides/fibre-fttc-ftth-broadband-guide.

[6] K. Witcher, "Fiber optics and its security vulnerabilities," *White Paper, SANS Institute,* 2005. [Online]. Available: https://www.giac.org/paper/gsec/4720/fiber-optics-security-vulnerabilities/106990.

[7] D. Kafura, "Cryptography: RSA Algorithm," Virginia Tech, 2000.

[8] ICO, "Guide to data protection: Encryption," Information Commissioner's Office, 2017. [Online]. Available: https://ico.org.uk/media/for-organisations/guide-to-data-protection/encryption-1-1.pdf

[9] M. Arora, "How secure is AES against brute force attacks," *EE Times,* vol. 5, no. 7, 2012. [Online]. Available: https://www.eetimes.com/how-secure-is-aes-against-brute-force-attacks/.

[10] NIST, "Advanced Encryption Standard (AES), Federal Inf. Process. Stds.," *(NIST FIPS) National Institute of Standards and Technology, Gaithersburg, MD,* 2001, doi: 10.6028/NIST.FIPS.197.

[11] Seagate Technology LLC, "128-Bit Versus 256-Bit AES Encryption," [Online] 2008. [Online]. Available: https://studylib.net/doc/18310732/128-bit-versus-256-bit-aes-encryption.

[12] L. K. Grover, "Quantum Mechanics Helps in Searching for a Needle in a Haystack," *Physical Review Letters,* vol. 79, no. 2, pp. 325-328, 1997, doi: 10.1103/PhysRevLett.79.325.

[13] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM,* vol. 21, no. 2, pp. 120-126, 1978, doi: 10.1145/359340.359342.

[14] E. Milanov, "The RSA algorithm," *RSA Laboratories,* pp. 1-11, 2009.

[15] C. Lily, M. Dustin, R. Karen, R. Andrew, and R. Angela, "Recommendations for Discrete Logarithm-based Cryptography: Elliptic Curve Domain Parameters," 2023, doi: 10.6028/NIST.SP.800-186.

[16] S. Ullah, J. Zheng, N. Din, M. T. Hussain, F. Ullah, and M. Yousaf, "Elliptic Curve Cryptography; Applications, challenges, recent advances, and future trends: A comprehensive survey," *Computer Science Review,* vol. 47, no. 100530, 2023, doi: 10.1016/j.cosrev.2022.100530.

[17] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," *Proceedings 35th Annual Symposium on Foundations of Computer Science,* pp. 124-134, 20-22 Nov. 1994, doi: 10.1109/SFCS.1994.365700.

[18] R. C. Johnson, "Quantum Computer May Crack Public-Key Encryption," *EE Times,* 2016.

[19] V. Gheorghiu and M. Mosca, "Benchmarking the quantum cryptanalysis of symmetric, public-key and hash-based cryptographic schemes," *arXiv,* pp. 1-19, 2019, doi: 10.48550/arXiv.1902.02332 [quant-ph].

[20] L. Chen, S. Jordan, Y.-K. Liu, D. Moody, R. Peralta, R. Perlner, and D. Smith-Tone, "Report on Post-Quantum Cryptography, NIST Interagency/Internal Report (NISTIR)," no. NISTIR 8105, pp. 1-16, 2016, doi: 10.6028/NIST.IR.8105.
[21] A. Gorjan, A. C. David, D. Quynh, D. Thinh, M. K. John, L. Jacob, L. Yi-Kai, A. M. Carl, M. Dustin, P. Rene, P. Ray, R. Angela, S.-T. Daniel, and A. Daniel, "Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process," 2022, doi: 10.6028/NIST.IR.8413.
[22] W. Heisenberg, "Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik," *Zeitschrift für Physik,* vol. 43, no. 3, pp. 172-198, 1927, doi: 10.1007/BF01397280.
[23] W. Heisenberg, "The actual content of quantum theoretical kinematics and mechanics," (in English), Translation vol. NASA TM-77379, no. 19840008978, pp. 1-33, 1983, doi: 10.1007/BF01397280. 1 December 1983.
[24] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature,* vol. 299, no. 5886, pp. 802-803, 1982, doi: 10.1038/299802a0.
[25] X.-B. Wang, T. Hiroshima, A. Tomita, and M. Hayashi, "Quantum information with Gaussian states," *Physics Reports,* vol. 448, no. 1, pp. 1-111, 2007, doi: 10.1016/j.physrep.2007.04.005.
[26] C. H. Bennett and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing," presented at the International Conference on Computers, Systems & Signal Processing, Bangalore, India, December 9-12, 1984.
[27] A. Carrasco-Casado, V. Fernández, and N. Denisenko, "Free-Space Quantum Key Distribution," in *Optical Wireless Communications: An Emerging Technology*, M. Uysal, C. Capsoni, Z. Ghassemlooy, A. Boucouvalas, and E. Udvary Eds. Cham: Springer International Publishing, 2016, pp. 589-607.
[28] M. N. Wegman and J. L. Carter, "New hash functions and their use in authentication and set equality," *Journal of Computer and System Sciences,* vol. 22, no. 3, pp. 265-279, 1981, doi: 10.1016/0022-0000(81)90033-7.
[29] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Reviews of Modern Physics,* vol. 74, no. 1, p. 145, 2002, doi: 10.1103/RevModPhys.74.145.
[30] P. W. Shor and J. Preskill, "Simple Proof of Security of the BB84 Quantum Key Distribution Protocol," *Physical Review Letters,* vol. 85, no. 2, pp. 441-444, 2000, doi: 10.1103/PhysRevLett.85.441.
[31] D. Elkouss, A. Leverrier, R. Alléaume, and J. J. Boutros, "Efficient reconciliation protocol for discrete-variable quantum key distribution," in *2009 IEEE International Symposium on Information Theory*, 2009: IEEE, pp. 1879-1883, doi: 10.1109/ISIT.2009.5205475.
[32] Y. Ding, D. Bacco, K. Dalgaard, X. Cai, X. Zhou, K. Rottwitt, and L. K. Oxenløwe, "High-dimensional quantum key distribution based on multicore fiber using silicon photonic integrated circuits," *npj Quantum Information,* vol. 3, no. 1, p. 25, 2017, doi: 10.1038/s41534-017-0026-2.
[33] B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C* John Wiley & Sons Inc., 1996.
[34] D. Mayers, "Unconditional security in Quantum Cryptography," *Journal of the Association for Computing Machinery,* vol. 48, no. 3, pp. 351-406, May 2001, doi: 10.1145/382780.382781.
[35] D. Mayers, "Shor and Preskill's and Mayers's security proof for the BB84 quantum key distribution protocol," *The European Physical Journal D - Atomic, Molecular, Optical and Plasma Physics,* vol. 18, no. 2, pp. 161-170, 2002, doi: 10.1140/epjd/e20020020.
[36] D. Gottesman, H. K. Lo, N. Lutkenhaus, and J. Preskill, "Security of quantum key distribution with imperfect devices," in *International Symposium onInformation*

Theory, 2004. ISIT 2004. Proceedings., 27 June-2 July 2004, p. 136, doi: 10.1109/ISIT.2004.1365172.

[37] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. Shamsul Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, "Advances in quantum cryptography," *Advances in Optics and Photonics,* vol. 12, no. 4, pp. 1012-1236, 2020, doi: 10.1364/AOP.361502.

[38] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J.-W. Pan, "Secure quantum key distribution with realistic devices," *Reviews of Modern Physics,* vol. 92, no. 025002, 2020, doi: 10.1103/RevModPhys.92.025002.

[39] H.-K. Lo, H. F. Chau, and M. Ardehali, "Efficient Quantum Key Distribution Scheme and a Proof of Its Unconditional Security," *Journal of Cryptology,* vol. 18, no. 2, pp. 133-165, 2005, doi: 10.1007/s00145-004-0142-y.

[40] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," *Physical Review Letters,* vol. 68, no. 21, pp. 3121-3124, 1992, doi: 10.1103/PhysRevLett.68.3121.

[41] K. Tamaki and N. Lütkenhaus, "Unconditional security of the Bennett 1992 quantum key-distribution protocol over a lossy and noisy channel," *Physical Review A,* vol. 69, no. 032316, 2004, doi: 10.1103/PhysRevA.69.032316.

[42] R. Renner, N. Gisin, and B. Kraus, "Information-theoretic security proof for quantum-key-distribution protocols," *Physical Review A,* vol. 72, no. 012332, 2005, doi: 10.1103/PhysRevA.72.012332.

[43] D. Bruß, "Optimal Eavesdropping in Quantum Cryptography with Six States," *Physical Review Letters,* vol. 81, no. 14, pp. 3018-3021, 1998, doi: 10.1103/PhysRevLett.81.3018.

[44] H. Bechmann-Pasquinucci and N. Gisin, "Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography," *Physical Review A,* vol. 59, no. 6, pp. 4238-4248, 1999, doi: 10.1103/PhysRevA.59.4238.

[45] G. Kato and K. Tamaki, "Security of six-state quantum key distribution protocol with threshold detectors," *Scientific Reports,* vol. 6, no. 30044, 2016, doi: 10.1038/srep30044.

[46] V. Scarani, A. Acín, G. Ribordy, and N. Gisin, "Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations," *Physical Review Letters,* vol. 92, no. 057901, 2004, doi: 10.1103/PhysRevLett.92.057901.

[47] C. Branciard, N. Gisin, B. Kraus, and V. Scarani, "Security of two quantum cryptography protocols using the same four qubit states," *Physical Review A,* vol. 72, no. 032301, 2005, doi: 10.1103/PhysRevA.72.032301.

[48] A. Laing, V. Scarani, J. G. Rarity, and J. L. O'Brien, "Reference-frame-independent quantum key distribution," *Physical Review A,* vol. 82, no. 012304, 2010, doi: 10.1103/PhysRevA.82.012304.

[49] T. Pramanik, B. K. Park, Y.-W. Cho, S.-W. Han, Y.-S. Kim, and S. Moon, "Robustness of reference-frame-independent quantum key distribution against the relative motion of the reference frames," *Physics Letters A,* vol. 381, no. 31, pp. 2497-2501, 2017, doi: 10.1016/j.physleta.2017.06.002.

[50] A. Carrasco-Casado, H. Kunimori, H. Takenaka, T. Kubo-Oka, M. Akioka, T. Fuse, Y. Koyama, D. Kolev, Y. Munemasa, and M. Toyoshima, "LEO-to-ground polarization measurements aiming for space QKD using Small Optical TrAnsponder (SOTA)," *Optics Express,* vol. 24, no. 11, pp. 12254-12266, 2016, doi: 10.1364/OE.24.012254.

[51] H. Takenaka, A. Carrasco-Casado, M. Fujiwara, M. Kitamura, M. Sasaki, and M. Toyoshima, "Satellite-to-ground quantum-limited communication using a 50-kg-class

microsatellite," *Nature Photonics,* vol. 11, no. 8, pp. 502-508, 2017, doi: 10.1038/nphoton.2017.107.
[52] A. Carrasco-Casado, H. Takenaka, D. Kolev, Y. Munemasa, H. Kunimori, K. Suzuki, T. Fuse, T. Kubo-Oka, M. Akioka, Y. Koyama, and M. Toyoshima, "LEO-to-ground optical communications using SOTA (Small Optical TrAnsponder) – Payload verification results and experiments on space quantum communications," *Acta Astronautica,* vol. 139, pp. 377-384, 2017, doi: 10.1016/j.actaastro.2017.07.030.
[53] A. Carrasco-Casado, H. Takenaka, M. Fujiwara, M. Kitamura, M. Sasaki, and M. Toyoshima, "QKD from a microsatellite: the SOTA experience," *SPIE Commercial + Scientific Sensing and Imaging,* vol. 10660, 2018, doi: 10.1117/12.2309624.
[54] Y. Xue, L. Shi, J. Wei, L. Yu, H. Yu, J. Tang, and Z. Zhang, "Reference-Frame-Independent Quantum Key Distribution in Uplink and Downlink Free-Space Channel," *International Journal of Theoretical Physics,* vol. 59, no. 10, pp. 3299-3309, 2020, doi: 10.1007/s10773-020-04587-x.
[55] H. Chun, I. Choi, G. Faulkner, L. Clarke, B. Barber, G. George, C. Capon, A. Niskanen, J. Wabnig, and D. O'Brien, "Handheld free space quantum key distribution with dynamic motion compensation," *Optics Express,* vol. 25, no. 6, pp. 6784-6795, 2017, doi: 10.1364/OE.25.006784.
[56] J. Wabnig, D. Bitauld, H. Li, A. Laing, J. O'Brien, and A. Niskanen, "Demonstration of free-space reference frame independent quantum key distribution," *New Journal of Physics,* vol. 15, no. 7, p. 073001, 2013, doi: 10.1088/1367-2630/15/7/073001.
[57] I. B. Djordjevic, *Physical-Layer Security and Quantum Key Distribution*, 1 ed. Springer Nature Switzerland AG 2019: Springer Cham, 2019.
[58] N. J. Cerf, M. Lévy, and G. V. Assche, "Quantum distribution of Gaussian keys using squeezed states," *Physical Review A,* vol. 63, no. 5, p. 052311, 2001, doi: 10.1103/PhysRevA.63.052311.
[59] F. Grosshans and P. Grangier, "Continuous Variable Quantum Cryptography Using Coherent States," *Physical Review Letters,* vol. 88, no. 057902, 2002, doi: 10.1103/PhysRevLett.88.057902.
[60] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Reviews of Modern Physics,* vol. 81, no. 3, pp. 1301-1350, 2009, doi: 10.1103/RevModPhys.81.1301.
[61] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, "Quantum key distribution using gaussian-modulated coherent states," *Nature,* vol. 421, no. 6920, pp. 238-241, 2003, doi: 10.1038/nature01289.
[62] F. Laudenbach, C. Pacher, C.-H. F. Fung, A. Poppe, M. Peev, B. Schrenk, M. Hentschel, P. Walther, and H. Hübel, "Continuous-Variable Quantum Key Distribution with Gaussian Modulation—The Theory of Practical Implementations," *Advanced Quantum Technologies,* vol. 1, no. 1800011, 2018, doi: 10.1002/qute.201800011.
[63] T. Ikuta and K. Inoue, "Intensity modulation and direct detection quantum key distribution based on quantum noise," *New Journal of Physics,* vol. 18, no. 013018, 2016, doi: 10.1088/1367-2630/18/1/013018.
[64] Y. Wang, X. Wu, L. Zhang, D. Huang, Q. Liao, and Y. Guo, "Performance improvement of free-space continuous-variable quantum key distribution with an adaptive optics unit," *Quantum Information Processing,* vol. 18, no. 8, p. 251, 2019, doi: 10.1007/s11128-019-2360-0.
[65] S. Wang, P. Huang, M. Liu, T. Wang, P. Wang, and G. Zeng, "Phase compensation for free-space continuous-variable quantum key distribution," *Optics Express,* vol. 28, no. 8, pp. 10737-10745, 2020, doi: 10.1364/OE.387402.
[66] N. Hosseinidehaj, Z. Babar, R. Malaney, S. X. Ng, and L. Hanzo, "Satellite-Based Continuous-Variable Quantum Communications: State-of-the-Art and a Predictive

Outlook," *IEEE Communications Surveys & Tutorials,* vol. 21, no. 1, pp. 881-919, 2019, doi: 10.1109/COMST.2018.2864557.
[67] T. Gonzalez-Raya, S. Pirandola, and M. Sanz, "Satellite-based entanglement distribution and quantum teleportation with continuous variables," *Communications Physics,* vol. 7, no. 1, p. 126, 2024, doi: 10.1038/s42005-024-01612-x.
[68] L. Mazzarella, C. Lowe, D. Lowndes, S. K. Joshi, S. Greenland, D. McNeil, C. Mercury, M. Macdonald, J. Rarity, and D. K. L. Oi, "QUARC: Quantum Research Cubesat—A Constellation for Quantum Communication," *Cryptography,* vol. 4, no. 1, p. 7, 2020, doi: 10.3390/cryptography4010007.
[69] I. Dror, A. Sandrov, and N. S. Kopeika, "Experimental investigation of the influence of the relative position of the scattering layer on image quality: the shower curtain effect," *Appl. Opt.,* vol. 37, no. 27, pp. 6495-6499, 1998, doi: 10.1364/AO.37.006495.
[70] A. Aspect, J. F. Clauser, and A. Zeilinger, "The Nobel Prize in Physics 2022. Entangled states - from theory to technology," 1st ed: The Royal Swedish Academy of Sciences, 2022.
[71] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Physical Review Letters,* vol. 67, no. 6, pp. 661-663, 1991, doi: 10.1103/PhysRevLett.67.661.
[72] J. S. Bell, "On the Einstein Podolsky Rosen paradox," *Physics Physique Fizika,* vol. 1, no. 3, pp. 195-200, 1964, doi: 10.1103/PhysicsPhysiqueFizika.1.195.
[73] J. S. Bell, "Bertlmann's socks and the nature of reality," *Le Journal de Physique Colloques,* vol. 42, no. C2, pp. C2-41-C2-62, 1981, doi: 10.1051/jphyscol:1981202.
[74] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, "Proposed Experiment to Test Local Hidden-Variable Theories," *Physical Review Letters,* vol. 23, no. 15, pp. 880-884, 1969, doi: 10.1103/PhysRevLett.23.880.
[75] A. Aspect, J. Dalibard, and G. Roger, "Experimental Test of Bell's Inequalities Using Time-Varying Analyzers," *Physical Review Letters,* vol. 49, no. 25, pp. 1804-1807, 1982, doi: 10.1103/PhysRevLett.49.1804.
[76] R. A. Bertlmann, "Bell's theorem and the nature of reality," *Foundations of Physics,* vol. 20, no. 10, pp. 1191-1212, 1990, doi: 10.1007/BF01889465.
[77] N. Ilic, "The ekert protocol," *Journal of Phy334,* vol. 1, pp. 1-4, 22 July 2007.
[78] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge: Cambridge University Press, 2010.
[79] J. F. Clauser and A. Shimony, "Bell's theorem. Experimental tests and implications," *Reports on Progress in Physics,* vol. 41, no. 12, p. 1881, 1978, doi: 10.1088/0034-4885/41/12/002.
[80] A. Peres, *Quantum theory: concepts and methods*. Springer, 1997.
[81] A. Ling, M. Peloso, I. Marcikic, A. Lamas-Linares, and C. Kurtsiefer, "Experimental E91 quantum key distribution," *Integrated Optoelectronic Devices 2008,* vol. 6903, 2008, doi: 10.1117/12.778556.
[82] F. Basso Basset, M. Valeri, E. Roccia, V. Muredda, D. Poderini, J. Neuwirth, N. Spagnolo, M. B. Rota, G. Carvacho, F. Sciarrino, and R. Trotta, "Quantum key distribution with entangled photons generated on demand by a quantum dot," *Science Advances,* vol. 7, no. 12, 2021, doi: 10.1126/sciadv.abe6379.
[83] A. Ling, M. P. Peloso, I. Marcikic, V. Scarani, A. Lamas-Linares, and C. Kurtsiefer, "Experimental quantum key distribution based on a Bell test," *Physical Review A,* vol. 78, no. 020301, 2008, doi: 10.1103/PhysRevA.78.020301.
[84] F. Basso Basset, M. Valeri, J. Neuwirth, E. Polino, M. B. Rota, D. Poderini, C. Pardo, G. Rodari, E. Roccia, S. F. Covre da Silva, G. Ronco, N. Spagnolo, A. Rastelli, G. Carvacho, F. Sciarrino, and R. Trotta, "Daylight entanglement-based quantum key distribution with a quantum dot source," *Quantum Science and Technology,* vol. 8, no. 025002, 2023, doi: 10.1088/2058-9565/acae3d.

[85] C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without Bell's theorem," *Physical Review Letters,* vol. 68, no. 5, pp. 557-559, 1992, doi: 10.1103/PhysRevLett.68.557.
[86] R. Bedington, J. M. Arrazola, and A. Ling, "Progress in satellite quantum key distribution," *npj Quantum Information,* vol. 3, no. 1, p. 30, 2017, doi: 10.1038/s41534-017-0031-5.
[87] M. P. Peloso, I. Gerhardt, C. Ho, A. Lamas-Linares, and C. Kurtsiefer, "Daylight operation of a free space, entanglement-based quantum key distribution system," *New Journal of Physics,* vol. 11, no. 045007, 2009, doi: 10.1088/1367-2630/11/4/045007.
[88] C. Erven, C. Couteau, R. Laflamme, and G. Weihs, "Entangled quantum key distribution over two free-space optical links," *Optics Express,* vol. 16, no. 21, pp. 16840-16853, 2008, doi: 10.1364/OE.16.016840.
[89] Y. Cao, H. Liang, J. Yin, H.-L. Yong, F. Zhou, Y.-P. Wu, J.-G. Ren, Y.-H. Li, G.-S. Pan, T. Yang, X. Ma, C.-Z. Peng, and J.-W. Pan, "Entanglement-based quantum key distribution with biased basis choice via free space," *Optics Express,* vol. 21, no. 22, pp. 27260-27268, 2013, doi: 10.1364/OE.21.027260.
[90] S. Mishra, A. Biswas, S. Patil, P. Chandravanshi, V. Mongia, T. Sharma, A. Rani, S. Prabhakar, S. Ramachandran, and R. P. Singh, "BBM92 quantum key distribution over a free space dusty channel of 200 meters," *Journal of Optics,* vol. 24, no. 7, p. 074002, 2022, doi: 10.1088/2040-8986/ac6f0b.
[91] H.-K. Lo, M. Curty, and B. Qi, "Measurement-Device-Independent Quantum Key Distribution," *Physical Review Letters,* vol. 108, no. 13, p. 130503, 2012, doi: 10.1103/PhysRevLett.108.130503.
[92] B. Qi, H. K. Lo, C. C. W. Lim, G. Siopsis, E. A. Chitambar, R. Pooser, P. G. Evans, and W. Grice, "Free-space reconfigurable quantum key distribution network," *2015 IEEE International Conference on Space Optical Systems and Applications (ICSOS),* pp. 1-6, 26-28 Oct. 2015, doi: 10.1109/ICSOS.2015.7425063.
[93] G. L. Roberts, M. Lucamarini, Z. L. Yuan, J. F. Dynes, L. C. Comandar, A. W. Sharpe, A. J. Shields, M. Curty, I. V. Puthoor, and E. Andersson, "Reconfigurable network for quantum digital signatures mediated by measurement-device-independent quantum key distribution," *QCrypt,* 2017.
[94] Y.-L. Tang, H.-L. Yin, Q. Zhao, H. Liu, X.-X. Sun, M.-Q. Huang, W.-J. Zhang, S.-J. Chen, L. Zhang, L.-X. You, Z. Wang, Y. Liu, C.-Y. Lu, X. Jiang, X. Ma, Q. Zhang, T.-Y. Chen, and J.-W. Pan, "Measurement-Device-Independent Quantum Key Distribution over Untrustful Metropolitan Network," *Physical Review X,* vol. 6, no. 1011024, 2016, doi: 10.1103/PhysRevX.6.011024.
[95] Y. Cao, Y.-H. Li, K.-X. Yang, Y.-F. Jiang, S.-L. Li, X.-L. Hu, M. Abulizi, C.-L. Li, W. Zhang, Q.-C. Sun, W.-Y. Liu, X. Jiang, S.-K. Liao, J.-G. Ren, H. Li, L. You, Z. Wang, J. Yin, C.-Y. Lu, X.-B. Wang, Q. Zhang, C.-Z. Peng, and J.-W. Pan, "Long-Distance Free-Space Measurement-Device-Independent Quantum Key Distribution," *Physical Review Letters,* vol. 125, no. 26, p. 260503, 2020, doi: 10.1103/PhysRevLett.125.260503.
[96] K. Inoue, E. Waks, and Y. Yamamoto, "Differential phase-shift quantum key distribution," *Photonics Asia,* vol. 4917, 2002, doi: 10.1117/12.483037.
[97] K. Inoue, E. Waks, and Y. Yamamoto, "Differential-phase-shift quantum key distribution using coherent light," *Physical Review A,* vol. 68, no. 022317, 2003, doi: 10.1103/PhysRevA.68.022317.
[98] K. Inoue, "Differential Phase-Shift Quantum Key Distribution Systems," *IEEE Journal of Selected Topics in Quantum Electronics,* vol. 21, no. 3, pp. 109-115, 2015, doi: 10.1109/JSTQE.2014.2360362.

[99] D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, "Fast and simple one-way quantum key distribution," *Applied Physics Letters,* vol. 87, no. 19, p. 194108, 2005, doi: 10.1063/1.2126792.
[100] D. Stucki, S. Fasel, N. Gisin, Y. Thoma, and H. Zbinden, "Coherent one-way quantum key distribution," *International Congress on Optics and Optoelectronics,* vol. 6583, 2007, doi: 10.1117/12.722952.
[101] D. Stucki, C. Barreiro, S. Fasel, J.-D. Gautier, O. Gay, N. Gisin, R. Thew, Y. Thoma, P. Trinkler, F. Vannel, and H. Zbinden, "Continuous high speed coherent one-way quantum key distribution," *Optics Express,* vol. 17, no. 16, pp. 13326-13334, 2009, doi: 10.1364/OE.17.013326.
[102] R. Trényi and M. Curty, "Zero-error attack against coherent-one-way quantum key distribution," *New Journal of Physics,* vol. 23, no. 9, p. 093005, 2021, doi: 10.1088/1367-2630/ac1e41.
[103] O. Alia, A. Schreier, R. Wang, S. Bahrani, R. Singh, G. Faulkner, J. Rarity, D. O'Brien, G. T. Kanellos, R. Nejabati, and D. Simeonidou, "DV-QKD Coexistence With 1.6 Terabit/s Classical Channels in Free Space Using Fiber-Wireless-Fiber Terminals," *European Conference on Optical Communication (ECOC) 2022,* p. Tu5.67, 2022.
[104] C. H. Bennett and G. Brassard, "Experimental quantum cryptography: the dawn of a new era for quantum cryptography: the experimental prototype is working!," *SIGACT News,* vol. 20, pp. 78-80, 1989, doi: 10.1145/74074.74087.
[105] M. Rau, T. Heindel, S. Unsleber, T. Braun, J. Fischer, S. Frick, S. Nauerth, C. Schneider, G. Vest, S. Reitzenstein, M. Kamp, A. Forchel, S. Höfling, and H. Weinfurter, "Free space quantum key distribution over 500 meters using electrically driven quantum dot single-photon sources—a proof of principle experiment," *New Journal of Physics,* vol. 16, no. 043003, 2014, doi: 10.1088/1367-2630/16/4/043003.
[106] D. A. Vajner, L. Rickert, T. Gao, K. Kaymazlar, and T. Heindel, "Quantum Communication Using Semiconductor Quantum Dots," *Advanced Quantum Technologies,* vol. 5, no. 7, p. 2100116, 2022, doi: 10.1002/qute.202100116.
[107] S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, and Z.-P. Li, "Satellite-to-ground quantum key distribution," *Nature,* vol. 549, no. 7670, p. 43, 2017, doi: 10.1038/nature23655.
[108] S.-K. Liao, H.-L. Yong, C. Liu, G.-L. Shentu, D.-D. Li, J. Lin, H. Dai, S.-Q. Zhao, B. Li, J.-Y. Guan, W. Chen, Y.-H. Gong, Y. Li, Z.-H. Lin, G.-S. Pan, J. S. Pelc, M. M. Fejer, W.-Z. Zhang, W.-Y. Liu, J. Yin, J.-G. Ren, X.-B. Wang, Q. Zhang, C.-Z. Peng, and J.-W. Pan, "Long-distance free-space quantum key distribution in daylight towards inter-satellite communication," *Nature Photonics,* vol. 11, no. 8, pp. 509-513, 2017, doi: 10.1038/nphoton.2017.116.
[109] W. T. Buttler, R. J. Hughes, P. G. Kwiat, G. G. Luther, G. L. Morgan, J. E. Nordholt, C. G. Peterson, and C. M. Simmons, "Free-space quantum-key distribution," *Physical Review A,* vol. 57, no. 4, pp. 2379-2382, 1998, doi: 10.1103/PhysRevA.57.2379.
[110] W. T. Buttler, R. J. Hughes, P. G. Kwiat, S. K. Lamoreaux, G. G. Luther, G. L. Morgan, J. E. Nordholt, C. G. Peterson, and C. M. Simmons, "Free-space quantum key distribution at night," *Aerospace/Defense Sensing and Controls,* vol. 3385, 1998, doi: 10.1117/12.312638.
[111] W. T. Buttler, R. J. Hughes, P. G. Kwiat, S. K. Lamoreaux, G. G. Luther, G. L. Morgan, J. E. Nordholt, C. G. Peterson, and C. M. Simmons, "Practical free-space quantum key distribution over 1 km," *Physical Review Letters,* vol. 81, no. 15, p. 3283, 1998, doi: 10.1103/PhysRevLett.81.3283.
[112] R. J. Hughes, W. T. Buttler, P. G. Kwiat, S. K. Lamoreaux, G. L. Morgan, J. E. Nordholt, and C. G. Peterson, "Practical quantum cryptography for secure free-space

communications," *arXiv:quant-ph/9905009,* 1999, doi: 10.48550/arXiv.quant-ph/9905009.
[113] R. J. Hughes, W. T. Buttler, P. G. Kwiat, S. K. Lamoreaux, G. G. Luther, G. L. Morgan, J. E. Nordholt, C. G. Peterson, and C. M. Simmons, "Practical Free-Space Quantum Cryptography," in *Proc. SPIE 3615, Free-Space Laser Communication Technologies XI*, 1999, vol. 3615, pp. 98-103, doi: 10.1117/12.346170.
[114] R. J. Hughes, J. E. Nordholt, D. Derkacs, and C. G. Peterson, "Practical free-space quantum key distribution over 10 km in daylight and at night," *New journal of physics,* vol. 4, no. 1, p. 43, 2002, doi: 10.1088/1367-2630/4/1/343.
[115] B. Jacobs and J. Franson, "Quantum cryptography in free space," *Optics Letters,* vol. 21, no. 22, pp. 1854-1856, 1996, doi: 10.1364/OL.21.001854.
[116] D. M. Benton, P. M. Gorman, P. R. Tapster, and D. M. Taylor, "A compact free space quantum key distribution system capable of daylight operation," *Optics Communications,* vol. 283, no. 11, pp. 2465-2471, 2010, doi: 10.1016/j.optcom.2009.10.039.
[117] W. T. Buttler, R. J. Hughes, S. K. Lamoreaux, G. L. Morgan, J. E. Nordholt, and C. G. Peterson, "Daylight Quantum Key Distribution over 1.6 km," *Physical Review Letters,* vol. 84, no. 24, pp. 5652-5655, 2000, doi: 10.1103/PhysRevLett.84.5652.
[118] H. Ko, K.-J. Kim, J.-S. Choe, B.-S. Choi, J.-H. Kim, Y. Baek, and C. J. Youn, "Experimental filtering effect on the daylight operation of a free-space quantum key distribution," *Scientific Reports,* vol. 8, no. 1, p. 15315, 2018, doi: 10.1038/s41598-018-33699-y.
[119] H. Weier, T. Schmitt-Manderbach, N. Regner, C. Kurtsiefer, and H. Weinfurter, "Free space quantum key distribution: Towards a real life application," *Fortschritte der Physik,* vol. 54, no. 8-10, pp. 840-845, 2006, doi: 10.1002/prop.200610322.
[120] M. J. García-Martínez, N. Denisenko, D. Soto, D. Arroyo, A. B. Orue, and V. Fernandez, "High-speed free-space quantum key distribution system for urban daylight applications," *Appl. Opt.,* vol. 52, no. 14, pp. 3311-3317, 2013, doi: 10.1364/AO.52.003311.
[121] F. Tang, S. Gao, X. Wang, and B. Zhu, "A novel synchronization scheme for free-space quantum key distribution system," *2011 Asia Communications and Photonics Conference and Exhibition (ACP),* pp. 1-7, 2011, doi: 10.1117/12.917952.
[122] C. Elliott, A. Colvin, D. Pearson, O. Pikalo, J. Schlafer, and H. Yeh, "Current status of the DARPA quantum network," *Defense and Security,* vol. 5815, 2005, doi: 10.1117/12.606489.
[123] M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. F. Dynes, S. Fasel, S. Fossier, M. Fürst, J. D. Gautier, O. Gay, N. Gisin, P. Grangier, A. Happe, Y. Hasani, M. Hentschel, H. Hübel, G. Humer, T. Länger, M. Legré, R. Lieger, J. Lodewyck, T. Lorünser, N. Lütkenhaus, A. Marhold, T. Matyus, O. Maurhart, L. Monat, S. Nauerth, J. B. Page, A. Poppe, E. Querasser, G. Ribordy, S. Robyr, L. Salvail, A. W. Sharpe, A. J. Shields, D. Stucki, M. Suda, C. Tamas, T. Themel, R. T. Thew, Y. Thoma, A. Treiber, P. Trinkler, R. Tualle-Brouri, F. Vannel, N. Walenta, H. Weier, H. Weinfurter, I. Wimberger, Z. L. Yuan, H. Zbinden, and A. Zeilinger, "The SECOQC quantum key distribution network in Vienna," *New Journal of Physics,* vol. 11, no. 075001, 2009, doi: 10.1088/1367-2630/11/7/075001.
[124] T.-Y. Chen, H. Liang, Y. Liu, W.-Q. Cai, L. Ju, W.-Y. Liu, J. Wang, H. Yin, K. Chen, Z.-B. Chen, C.-Z. Peng, and J.-W. Pan, "Field test of a practical secure communication network with decoy-state quantum cryptography," *Optics Express,* vol. 17, no. 8, pp. 6540-6549, 2009, doi: 10.1364/OE.17.006540.
[125] T.-Y. Chen, J. Wang, H. Liang, W.-Y. Liu, Y. Liu, X. Jiang, Y. Wang, X. Wan, W.-Q. Cai, L. Ju, L.-K. Chen, L.-J. Wang, Y. Gao, K. Chen, C.-Z. Peng, Z.-B. Chen, and J.-

W. Pan, "Metropolitan all-pass and inter-city quantum communication network," *Optics Express,* vol. 18, no. 26, pp. 27217-27225, 2010, doi: 10.1364/OE.18.027217.

[126] S. Wang, W. Chen, Z.-Q. Yin, H.-W. Li, D.-Y. He, Y.-H. Li, Z. Zhou, X.-T. Song, F.-Y. Li, D. Wang, H. Chen, Y.-G. Han, J.-Z. Huang, J.-F. Guo, P.-L. Hao, M. Li, C.-M. Zhang, D. Liu, W.-Y. Liang, C.-H. Miao, P. Wu, G.-C. Guo, and Z.-F. Han, "Field and long-term demonstration of a wide area quantum key distribution network," *Optics Express,* vol. 22, no. 18, pp. 21739-21756, 2014, doi: 10.1364/OE.22.021739.

[127] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumaru, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, A. W. Sharpe, Z. L. Yuan, A. J. Shields, S. Uchikoga, M. Legré, S. Robyr, P. Trinkler, L. Monat, J. B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Länger, M. Peev, and A. Zeilinger, "Field test of quantum key distribution in the Tokyo QKD Network," *Optics Express,* vol. 19, no. 11, pp. 10387-10409, 2011, doi: 10.1364/OE.19.010387.

[128] S. Nauerth, F. Moll, M. Rau, C. Fuchs, J. Horwath, S. Frick, and H. Weinfurter, "Air-to-ground quantum communication," *Nature Photonics,* vol. 7, no. 5, pp. 382-386, 2013, doi: 10.1038/nphoton.2013.46.

[129] J.-Y. Wang, B. Yang, S.-K. Liao, L. Zhang, Q. Shen, X.-F. Hu, J.-C. Wu, S.-J. Yang, H. Jiang, Y.-L. Tang, B. Zhong, H. Liang, W.-Y. Liu, Y.-H. Hu, Y.-M. Huang, B. Qi, J.-G. Ren, G.-S. Pan, J. Yin, J.-J. Jia, Y.-A. Chen, K. Chen, C.-Z. Peng, and J.-W. Pan, "Direct and full-scale experimental verifications towards ground–satellite quantum key distribution," *Nature Photonics,* vol. 7, no. 5, pp. 387-393, 2013, doi: 10.1038/nphoton.2013.89.

[130] S.-K. Liao, W.-Q. Cai, J. Handsteiner, B. Liu, J. Yin, L. Zhang, D. Rauch, M. Fink, J.-G. Ren, W.-Y. Liu, Y. Li, Q. Shen, Y. Cao, F.-Z. Li, J.-F. Wang, Y.-M. Huang, L. Deng, T. Xi, L. Ma, T. Hu, L. Li, N.-L. Liu, F. Koidl, P. Wang, Y.-A. Chen, X.-B. Wang, M. Steindorfer, G. Kirchner, C.-Y. Lu, R. Shu, R. Ursin, T. Scheidl, C.-Z. Peng, J.-Y. Wang, A. Zeilinger, and J.-W. Pan, "Satellite-Relayed Intercontinental Quantum Network," *Physical Review Letters,* vol. 120, no. 3, p. 030501, 2018, doi: 10.1103/PhysRevLett.120.030501.

[131] Y.-A. Chen, Q. Zhang, T.-Y. Chen, W.-Q. Cai, S.-K. Liao, J. Zhang, K. Chen, J. Yin, J.-G. Ren, Z. Chen, S.-L. Han, Q. Yu, K. Liang, F. Zhou, X. Yuan, M.-S. Zhao, T.-Y. Wang, X. Jiang, L. Zhang, W.-Y. Liu, Y. Li, Q. Shen, Y. Cao, C.-Y. Lu, R. Shu, J.-Y. Wang, L. Li, N.-L. Liu, F. Xu, X.-B. Wang, C.-Z. Peng, and J.-W. Pan, "An integrated space-to-ground quantum communication network over 4,600 kilometres," *Nature,* vol. 589, no. 7841, pp. 214-219, 2021, doi: 10.1038/s41586-020-03093-8.

[132] J. Duligall, M. Godfrey, K. Harrison, W. Munro, and J. Rarity, "Low cost and compact quantum key distribution," *New Journal of Physics,* vol. 8, no. 10, p. 249, 2006, doi: 10.1088/1367-2630/8/10/249.

[133] D. Lowndes, S. Frick, A. Hart, and J. Rarity, "A low cost, short range quantum key distribution system," *EPJ Quantum Technology,* vol. 8, no. 1, p. 15, 2021, doi: 10.1140/epjqt/s40507-021-00101-2.

[134] D. Lowndes, A. Schreier, D. O'Brien, and J. Rarity, "Characterising a handheld quantum key distribution system with emulated beam steering," *SPIE Photonex,* vol. 11881, 2021, doi: 10.1117/12.2603355.

[135] A. Schreier, O. Alia, R. Wang, R. Singh, G. Faulkner, G. Kanellos, R. Nejabati, D. Simeonidou, J. Rarity, and D. O. Brien, "Coexistence of Quantum and 1.6 Tbit/s Classical Data Over Fibre-Wireless-Fibre Terminals," *Journal of Lightwave Technology,* pp. 1-7, 2023, doi: 10.1109/JLT.2023.3258146.

[136] M. Avesani, L. Calderaro, M. Schiavon, A. Stanco, C. Agnesi, A. Santamato, M. Zahidy, A. Scriminich, G. Foletto, G. Contestabile, M. Chiesa, D. Rotta, M. Artiglia, A. Montanaro, M. Romagnoli, V. Sorianello, F. Vedovato, G. Vallone, and P. Villoresi, "Full daylight quantum-key-distribution at 1550 nm enabled by integrated silicon photonics," *npj Quantum Information,* vol. 7, no. 1, p. 93, 2021, doi: 10.1038/s41534-021-00421-2.

[137] Y.-H. Gong, K.-X. Yang, H.-L. Yong, J.-Y. Guan, G.-L. Shentu, C. Liu, F.-Z. Li, Y. Cao, J. Yin, S.-K. Liao, J.-G. Ren, Q. Zhang, C.-Z. Peng, and J.-W. Pan, "Free-space quantum key distribution in urban daylight with the SPGD algorithm control of a deformable mirror," *Optics Express,* vol. 26, no. 15, pp. 18897-18905, 2018, doi: 10.1364/OE.26.018897.

[138] A. Biswas, A. Banerji, P. Chandravanshi, R. Kumar, and R. P. Singh, "Experimental Side Channel Analysis of BB84 QKD Source," *IEEE Journal of Quantum Electronics,* vol. 57, no. 6, pp. 1-7, 2021, doi: 10.1109/JQE.2021.3111332.

[139] M. J. García-Martínez, N. Denisenko, D. Soto, and V. Fernández, "Towards a Short-range Free-space GHz-clocked Quantum Key Distribution System," in *International Conference on Quantum Information*, Ottawa, 2011: Optica Publishing Group, in OSA Technical Digest (CD), p. QMI17, doi: 10.1364/ICQI.2011.QMI17.

[140] R. Alléaume, F. Treussart, G. Messin, Y. Dumeige, J. F. Roch, A. Beveratos, R. Brouri-Tualle, J. P. Poizat, and P. Grangier, "Experimental open-air quantum key distribution with a single-photon source," *New Journal of Physics,* vol. 6, no. 1, p. 92, 2004, doi: 10.1088/1367-2630/6/1/092.

[141] T. Heindel, C. A. Kessler, M. Rau, C. Schneider, M. Fürst, F. Hargart, W.-M. Schulz, M. Eichfelder, R. Roßbach, S. Nauerth, M. Lermer, H. Weier, M. Jetter, M. Kamp, S. Reitzenstein, S. Höfling, P. Michler, H. Weinfurter, and A. Forchel, "Quantum key distribution using quantum dot single-photon emitting diodes in the red and near infrared spectral range," *New Journal of Physics,* vol. 14, no. 083001, 2012, doi: 10.1088/1367-2630/14/8/083001.

[142] G. Mélen, T. Vogl, M. Rau, G. Corrielli, A. Crespi, R. Osellame, and H. Weinfurter, "Integrated quantum key distribution sender unit for daily-life implementations," *Proc.SPIE,* vol. 9762, p. 97620A, 2016, doi: 10.1117/12.2208643.

[143] M. Rau, T. Vogl, G. Corrielli, G. Vest, L. Fuchs, S. Nauerth, and H. Weinfurter, "Spatial Mode Side Channels in Free-Space QKD Implementations," *IEEE Journal of Selected Topics in Quantum Electronics,* vol. 21, no. 3, pp. 187-191, 2015, doi: 10.1109/JSTQE.2014.2372008.

[144] G. Vest, P. Freiwang, J. Luhn, T. Vogl, M. Rau, L. Knips, W. Rosenfeld, and H. Weinfurter, "Quantum key Distribution with a Hand-Held Sender Unit," *Physical Review Applied,* vol. 18, no. 024067, 2022, doi: 10.1103/PhysRevApplied.18.024067.

[145] S. Nauerth, M. Fürst, T. Schmitt-Manderbach, H. Weier, and H. Weinfurter, "Information leakage via side channels in freespace BB84 quantum cryptography," *New Journal of Physics,* vol. 11, no. 6, p. 065001, 2009/06/03 2009, doi: 10.1088/1367-2630/11/6/065001.

[146] J. Rarity, P. Tapster, P. Gorman, and P. Knight, "Ground to satellite secure key exchange using quantum cryptography," *New Journal of Physics,* vol. 4, no. 1, p. 82, 2002, doi: 10.1088/1367-2630/4/1/382.

[147] T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, A. Zeilinger, and H. Weinfurter, "Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km," *Physical Review Letters,* vol. 98, no. 1, p. 010504, 2007, doi: 10.1103/PhysRevLett.98.010504.

[148] W. S. Rabinovich, R. Mahon, M. S. Ferraro, P. G. Goetz, M. Bashkansky, R. E. Freeman, J. Reintjes, and J. L. Murphy, "Free space quantum key distribution using

modulating retro-reflectors," *Optics Express,* vol. 26, no. 9, pp. 11331-11351, 2018, doi: 10.1364/OE.26.011331.
[149] C. Quintana, P. Sibson, G. Erry, Y. Thueux, E. Kingston, T. Ismail, G. Faulkner, J. Kennard, K. Gebremicael, C. Clark, C. Erven, S. Chuard, M. Watson, J. Rarity, and D. O'Brien, *Low size, weight and power quantum key distribution system for small form unmanned aerial vehicles* (SPIE LASE). SPIE, 2019.
[150] K. J. Resch, M. Lindenthal, B. Blauensteiner, H. R. Böhm, A. Fedrizzi, C. Kurtsiefer, A. Poppe, T. Schmitt-Manderbach, M. Taraba, R. Ursin, P. Walther, H. Weier, H. Weinfurter, and A. Zeilinger, "Distributing entanglement and single photons through an intra-city, free-space quantum channel," *Optics Express,* vol. 13, no. 1, pp. 202-209, 2005, doi: 10.1364/OPEX.13.000202.
[151] I. Marcikic, A. Lamas-Linares, and C. Kurtsiefer, "Free-space quantum key distribution with entangled photons," *Applied Physics Letters,* vol. 89, no. 10, p. 101122, 2006, doi: 10.1063/1.2348775.
[152] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Ömer, M. Fürst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, and A. Zeilinger, "Entanglement-based quantum communication over 144 km," *Nature Physics,* vol. 3, no. 7, pp. 481-486, 2007, doi: 10.1038/nphys629.
[153] J. Yin, Y.-H. Li, S.-K. Liao, M. Yang, Y. Cao, L. Zhang, J.-G. Ren, W.-Q. Cai, W.-Y. Liu, S.-L. Li, R. Shu, Y.-M. Huang, L. Deng, L. Li, Q. Zhang, N.-L. Liu, Y.-A. Chen, C.-Y. Lu, X.-B. Wang, F. Xu, J.-Y. Wang, C.-Z. Peng, A. K. Ekert, and J.-W. Pan, "Entanglement-based secure quantum cryptography over 1,120 kilometres," *Nature,* 2020/06/15 2020, doi: 10.1038/s41586-020-2401-y.
[154] S. Ecker, B. Liu, J. Handsteiner, M. Fink, D. Rauch, F. Steinlechner, T. Scheidl, A. Zeilinger, and R. Ursin, "Strategies for achieving high key rates in satellite-based QKD," *npj Quantum Information,* vol. 7, no. 1, p. 5, 2021, doi: 10.1038/s41534-020-00335-5.
[155] D. Stucki, M. Legré, F. Buntschu, B. Clausen, N. Felber, N. Gisin, L. Henzen, P. Junod, G. Litzistorf, P. Monbaron, L. Monat, J. B. Page, D. Perroud, G. Ribordy, A. Rochas, S. Robyr, J. Tavares, R. Thew, P. Trinkler, S. Ventura, R. Voirol, N. Walenta, and H. Zbinden, "Long-term performance of the SwissQuantum quantum key distribution network in a field environment," *New Journal of Physics,* vol. 13, no. 12, p. 123001, 2011, doi: 10.1088/1367-2630/13/12/123001.
[156] T. Jennewein, C. Grant, E. Choi, C. Pugh, C. Holloway, J. Bourgoin, H. Hakima, B. Higgins, and R. Zee, "The NanoQEY mission: ground to space quantum key and entanglement distribution using a nanosatellite," *Proc. SPIE 9254, Emerging Technologies in Security and Defence II; and Quantum- Physics-based Information Security III, 925402,* 2014, doi: 10.1117/12.2067548.
[157] R. Bedington, X. Bai, E. Truong-Cao, Y. C. Tan, K. Durak, A. Villar Zafra, J. A. Grieve, D. K. L. Oi, and A. Ling, "Nanosatellite experiments to enable future space-based QKD missions," *EPJ Quantum Technology,* vol. 3, no. 1, p. 12, 2016, doi: 10.1140/epjqt/s40507-016-0051-7.
[158] D. K. L. Oi, A. Ling, G. Vallone, P. Villoresi, S. Greenland, E. Kerr, M. Macdonald, H. Weinfurter, H. Kuiper, E. Charbon, and R. Ursin, "CubeSat quantum communications mission," *EPJ Quantum Technology,* vol. 4, no. 1, p. 6, 2017, doi: 10.1140/epjqt/s40507-017-0060-1.
[159] Z. Tang, R. Chandrasekara, Y. C. Tan, C. Cheng, L. Sha, G. C. Hiang, D. K. L. Oi, and A. Ling, "Generation and Analysis of Correlated Pairs of Photons aboard a Nanosatellite," *Physical Review Applied,* vol. 5, no. 054022, 2016, doi: 10.1103/PhysRevApplied.5.054022.

[160] M. Toyoshima, H. Takenaka, Y. Shoji, Y. Takayama, Y. Koyama, and H. Kunimori, "Polarization measurements through space-to-ground atmospheric propagation paths by using a highly polarized laser source in space," *Optics Express,* vol. 17, no. 25, pp. 22333-22340, 2009, doi: 10.1364/OE.17.022333.
[161] P. Villoresi, T. Jennewein, F. Tamburini, M. Aspelmeyer, C. Bonato, R. Ursin, C. Pernechele, V. Luceri, G. Bianco, A. Zeilinger, and C. Barbieri, "Experimental verification of the feasibility of a quantum channel between space and Earth," *New Journal of Physics,* vol. 10, no. 033038, 2008, doi: 10.1088/1367-2630/10/3/033038.
[162] J. Yin, Y. Cao, S.-B. Liu, G.-S. Pan, J.-H. Wang, T. Yang, Z.-P. Zhang, F.-M. Yang, Y.-A. Chen, C.-Z. Peng, and J.-W. Pan, "Experimental quasi-single-photon transmission from satellite to earth," *Optics Express,* vol. 21, no. 17, pp. 20032-20040, 2013, doi: 10.1364/OE.21.020032.
[163] G. Vallone, D. Bacco, D. Dequal, S. Gaiarin, V. Luceri, G. Bianco, and P. Villoresi, "Experimental Satellite Quantum Communications," *Physical Review Letters,* vol. 115, no. 040502, 2015, doi: 10.1103/PhysRevLett.115.040502.
[164] Q. Zhang, F. Xu, Y.-A. Chen, C.-Z. Peng, and J.-W. Pan, "Large scale quantum key distribution: challenges and solutions [Invited]," *Optics Express,* vol. 26, no. 18, pp. 24260-24273, 2018, doi: 10.1364/OE.26.024260.
[165] J. Yin, Y. Cao, Y.-H. Li, S.-K. Liao, L. Zhang, J.-G. Ren, W.-Q. Cai, W.-Y. Liu, B. Li, and H. Dai, "Satellite-based entanglement distribution over 1200 kilometers," *Science,* vol. 356, no. 6343, pp. 1140-1144, 2017, doi: 10.1126/science.aan3211.
[166] C.-Z. Peng, T. Yang, X.-H. Bao, J. Zhang, X.-M. Jin, F.-Y. Feng, B. Yang, J. Yang, J. Yin, Q. Zhang, N. Li, B.-L. Tian, and J.-W. Pan, "Experimental Free-Space Distribution of Entangled Photon Pairs Over 13 km: Towards Satellite-Based Global Quantum Communication," *Physical Review Letters,* vol. 94, no. 15, p. 150501, 2005, doi: 10.1103/PhysRevLett.94.150501.
[167] J.-G. Ren, P. Xu, H.-L. Yong, L. Zhang, S.-K. Liao, J. Yin, W.-Y. Liu, W.-Q. Cai, M. Yang, L. Li, K.-X. Yang, X. Han, Y.-Q. Yao, J. Li, H.-Y. Wu, S. Wan, L. Liu, D.-Q. Liu, Y.-W. Kuang, Z.-P. He, P. Shang, C. Guo, R.-H. Zheng, K. Tian, Z.-C. Zhu, N.-L. Liu, C.-Y. Lu, R. Shu, Y.-A. Chen, C.-Z. Peng, J.-Y. Wang, and J.-W. Pan, "Ground-to-satellite quantum teleportation," *Nature,* vol. 549, no. 7670, pp. 70-73, 2017, doi: 10.1038/nature23675.
[168] R. Singh, F. Feng, Y. Hong, G. Faulkner, R. Deshmukh, G. Vercasson, O. Bouchet, P. Petropoulos, and D. O'Brien, "Design and Characterisation of Terabit/s Capable Compact Localisation and Beam-Steering Terminals for Fiber-Wireless-Fiber Links," *Journal of Lightwave Technology,* vol. 38, no. 24, pp. 6817-6826, 2020, doi: 10.1109/JLT.2020.3022754.
[169] R. Singh, A. Schreier, G. Faulkner, and D. O'Brien, "Fiber-Wireless-Fiber Terminals for Optical Wireless Communication over Multiple Bands," *2020 IEEE Photonics Conference (IPC),* pp. 1-2, 28 Sept.-1 Oct. 2020, doi: 10.1109/IPC47351.2020.9252288.
[170] Y. Hong, F. Feng, K. R. H. Bottrill, N. Taengnoi, R. Singh, G. Faulkner, D. C. O'Brien, and P. Petropoulos, "Beyond Terabit/s WDM Optical Wireless Transmission using Wavelength-transparent Beam Tracking and Steering," *Optical Fiber Communication Conference (OFC) 2020,* p. W1G.4, 2020, doi: 10.1364/OFC.2020.W1G.4.
[171] Y. Hong, F. Feng, K. R. H. Bottrill, N. Taengnoi, R. Singh, G. Faulkner, D. C. O'Brien, and P. Petropoulos, "Demonstration of >1Tbit/s WDM OWC with wavelength-transparent beam tracking-and-steering capability," *Optics Express,* vol. 29, no. 21, pp. 33694-33702, 2021, doi: 10.1364/OE.436239.
[172] F. Feng, P. Sangwongngam, H. Chun, G. Faulkner, and D. O. Brien, "Optical Broadcasting for Wide Field-of-View Bidirectional Indoor Optical Wireless

Communications," *2019 Conference on Lasers and Electro-Optics (CLEO),* pp. 1-2, 5-10 May 2019, doi: 10.1364/CLEO_SI.2019.SM2G.5.
[173] F. Feng, P. Sangwongngam, G. E. Faulkner, and D. O'brien, "Wide field-of-view optical broadcasting for bi-directional indoor optical wireless communications employing PAM-4 modulation," *Optics letters,* vol. 44 24, pp. 6009-6012, 2019, doi: 10.1364/OL.44.006009.
[174] F. Feng, P. Sangwongngam, G. Faulkner, and D. O'Brien, "Wide Field-of-View Flexible Wavelength Routing and Multicasting for Multi-user Bi-directional Indoor Optical Wireless Communications," *Conference on Lasers and Electro-Optics,* p. STu4L.4, 2020, doi: 10.1364/CLEO_SI.2020.STu4L.4.
[175] F. Feng, P. Sangwongngam, H. Chun, G. Faulkner, and D. O'Brien, "Indoor Optical Wireless Communications with WDM-OFDMA Enabled by an Optical Hotspot with a Wide Field-of-View," *European Conference on Optical Communication (ECOC) 2022,* p. We3F.1, 2022.
[176] A. Gomez, K. Shi, C. Quintana, M. Sato, G. Faulkner, B. C. Thomsen, and D. O'Brien, "Beyond 100-Gb/s indoor wide field-of-view optical wireless communications," *IEEE Photonics Technology Letters,* vol. 27, no. 4, pp. 367-370, 2014, doi: 10.1109/LPT.2014.2374995.
[177] A. Gomez, K. Shi, C. Quintana, R. Maher, G. Faulkner, P. Bayvel, B. C. Thomsen, and D. O'Brien, "Design and demonstration of a 400 Gb/s indoor optical wireless communications link," *Journal of Lightwave Technology,* vol. 34, no. 22, pp. 5332-5339, 2016, doi: 10.1109/JLT.2016.2616844.
[178] A. Gomez, K. Shi, C. Quintana, G. Faulkner, B. C. Thomsen, and D. O'Brien, "A 50 Gb/s transparent indoor optical wireless communications link with an integrated localization and tracking system," *Journal of Lightwave Technology,* vol. 34, no. 10, pp. 2510-2517, 2016, doi: 10.1109/JLT.2016.2542158.
[179] C. A. Fuchs, N. Gisin, R. B. Griffiths, C.-S. Niu, and A. Peres, "Optimal eavesdropping in quantum cryptography. Information bound and optimal strategy," *Physical Review A,* vol. 56, no. 2, pp. 1163-1172, 1997, doi: 10.1103/PhysRevA.56.1163.
[180] B. Slutsky, R. Rao, P. C. Sun, and Y. Fainman, "Security of quantum cryptography against individual attacks," *SPIE Voice, Video, and Data Communications,* vol. 3228, 1998, doi: 10.1117/12.300902.
[181] N. Lütkenhaus, "Estimates for practical quantum cryptography," *Physical Review A,* vol. 59, no. 5, pp. 3301-3319, 1999, doi: 10.1103/PhysRevA.59.3301.
[182] N. Lütkenhaus, "Security against individual attacks for realistic quantum key distribution," *Physical Review A,* vol. 61, no. 052304, 2000, doi: 10.1103/PhysRevA.61.052304.
[183] T. Metger and R. Renner, "Security of quantum key distribution from generalised entropy accumulation," *Nature Communications,* vol. 14, no. 1, p. 5272, 2023, doi: 10.1038/s41467-023-40920-8.
[184] V. Scarani and R. Renner, "Quantum Cryptography with Finite Resources: Unconditional Security Bound for Discrete-Variable Protocols with One-Way Postprocessing," *Physical Review Letters,* vol. 100, no. 20, p. 200501, 2008, doi: 10.1103/PhysRevLett.100.200501.
[185] R. Y. Q. Cai and V. Scarani, "Finite-key analysis for practical implementations of quantum key distribution," *New Journal of Physics,* vol. 11, no. 4, p. 045024, 2009, doi: 10.1088/1367-2630/11/4/045024.
[186] Y. Sano, R. Matsumoto, and T. Uyematsu, "Secure key rate of the BB84 protocol using finite sample bits*," *Journal of Physics A: Mathematical and Theoretical,* vol. 43, no. 49, p. 495302, 2010, doi: 10.1088/1751-8113/43/49/495302.

[187] L. Sheridan and V. Scarani, "Security proof for quantum key distribution using qudit systems," *Physical Review A,* vol. 82, no. 3, p. 030301, 2010, doi: 10.1103/PhysRevA.82.030301.
[188] L. Sheridan, T. P. Le, and V. Scarani, "Finite-key security against coherent attacks in quantum key distribution," *New Journal of Physics,* vol. 12, no. 12, p. 123019, 2010, doi: 10.1088/1367-2630/12/12/123019.
[189] M. Hayashi and T. Tsurumaru, "Concise and tight security analysis of the Bennett–Brassard 1984 protocol with finite key lengths," *New Journal of Physics,* vol. 14, no. 9, p. 093014, 2012, doi: 10.1088/1367-2630/14/9/093014.
[190] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, "Tight finite-key analysis for quantum cryptography," *Nature Communications,* vol. 3, no. 1, p. 634, 2012, doi: 10.1038/ncomms1631.
[191] M. Tomamichel, J. Martinez-Mateo, C. Pacher, and D. Elkouss, "Fundamental finite key limits for one-way information reconciliation in quantum key distribution," *Quantum Information Processing,* vol. 16, no. 11, p. 280, 2017, doi: 10.1007/s11128-017-1709-5.
[192] N. Jain, B. Stiller, I. Khan, D. Elser, C. Marquardt, and G. Leuchs, "Attacks on practical quantum key distribution systems (and how to prevent them)," *Contemporary Physics,* vol. 57, no. 3, pp. 366-387, 2016, doi: 10.1080/00107514.2016.1148333.
[193] P. Arteaga-Díaz, D. Cano, and V. Fernandez, "Practical Side-Channel Attack on Free-Space QKD Systems With Misaligned Sources and Countermeasures," *IEEE Access,* vol. 10, pp. 82697-82705, 2022, doi: 10.1109/ACCESS.2022.3196677.
[194] H.-K. Lo, X. Ma, and K. Chen, "Decoy State Quantum Key Distribution," *Physical Review Letters,* vol. 94, no. 23, p. 230504, 2005, doi: 10.1103/PhysRevLett.94.230504.
[195] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, "Practical decoy state for quantum key distribution," *Physical Review A,* vol. 72, no. 012326, 2005, doi: 10.1103/PhysRevA.72.012326.
[196] H.-K. Lo, M. Curty, and K. Tamaki, "Secure quantum key distribution," *Nature Photonics,* vol. 8, no. 8, pp. 595-604, 2014, doi: 10.1038/nphoton.2014.149.
[197] X.-B. Wang, "Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography," *Physical Review Letters,* vol. 94, no. 23, p. 230503, 2005, doi: 10.1103/PhysRevLett.94.230503.
[198] X.-B. Wang, "Decoy-state protocol for quantum cryptography with four different intensities of coherent light," *Physical Review A,* vol. 72, no. 1, p. 012322, 2005, doi: 10.1103/PhysRevA.72.012322.
[199] J. W. Harrington, J. M. Ettinger, R. J. Hughes, and J. E. Nordholt, "Enhancing practical security of quantum key distribution with a few decoy states," *arXiv,* pp. 1-4, 2005, doi: 10.48550/arXiv.quant-ph/0503002.
[200] Y. Zhao, B. Qi, X. Ma, H. k. Lo, and L. Qian, "Simulation and Implementation of Decoy State Quantum Key Distribution over 60km Telecom Fiber," *2006 IEEE International Symposium on Information Theory,* pp. 2094-2098, 2006, doi: 10.1109/ISIT.2006.261920.
[201] X.-B. Wang, "Decoy-state quantum key distribution with large random errors of light intensity," *Physical Review A,* vol. 75, no. 5, p. 052301, 2007, doi: 10.1103/PhysRevA.75.052301.
[202] M. Hayashi, "General theory for decoy-state quantum key distribution with an arbitrary number of intensities," *New Journal of Physics,* vol. 9, no. 8, p. 284, 2007, doi: 10.1088/1367-2630/9/8/284.

[203] Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian, "Experimental Quantum Key Distribution with Decoy States," *Physical Review Letters,* vol. 96, no. 7, p. 070502, 2006, doi: 10.1103/PhysRevLett.96.070502.
[204] D. Rosenberg, J. W. Harrington, P. R. Rice, P. A. Hiskett, C. G. Peterson, R. J. Hughes, A. E. Lita, S. W. Nam, and J. E. Nordholt, "Long-Distance Decoy-State Quantum Key Distribution in Optical Fiber," *Physical Review Letters,* vol. 98, no. 1, p. 010503, 2007, doi: 10.1103/PhysRevLett.98.010503.
[205] C.-Z. Peng, J. Zhang, D. Yang, W.-B. Gao, H.-X. Ma, H. Yin, H.-P. Zeng, T. Yang, X.-B. Wang, and J.-W. Pan, "Experimental Long-Distance Decoy-State Quantum Key Distribution Based on Polarization Encoding," *Physical Review Letters,* vol. 98, no. 1, p. 010505, 2007, doi: 10.1103/PhysRevLett.98.010505.
[206] C. L. Morrison, R. G. Pousa, F. Graffitti, Z. X. Koong, P. Barrow, N. G. Stoltz, D. Bouwmeester, J. Jeffers, D. K. L. Oi, B. D. Gerardot, and A. Fedrizzi, "Single-emitter quantum key distribution over 175 km of fibre with optimised finite key rates," *Nature Communications,* vol. 14, no. 1, p. 3573, 2023/06/16 2023, doi: 10.1038/s41467-023-39219-5.
[207] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, "Fundamental limits of repeaterless quantum communications," *Nature Communications,* vol. 8, no. 1, p. 15043, 2017, doi: 10.1038/ncomms15043.
[208] I. N. Sokolik, "Absorption by atmospheric gases in the IR, visible and UV spectral regions," *School of Earth and Atmospheric Sciences, Georgia Institute of Technology,* 2009.
[209] VIAVI Solutions, "Fiber Water Peak Characterization," White Paper pp. 1-6, 2020. [Online]. Available: https://www.viavisolutions.com/en-us/literature/fiber-water-peak-characterization-white-papers-books-en.pdf.
[210] Corning, "Corning SMF-28 Ultra Optical Fiber," [Online] 2021. [Online]. Available: https://www.corning.com/media/worldwide/coc/documents/Fiber/product-information-sheets/PI-1424-AEN.pdf.
[211] W. Chen, Z. F. Han, T. Zhang, H. Wen, Z. Q. Yin, F. X. Xu, Q. L. Wu, Y. Liu, Y. Zhang, X. F. Mo, Y. Z. Gui, G. Wei, and G. C. Guo, "Field Experiment on a "Star Type" Metropolitan Quantum Key Distribution Network," *IEEE Photonics Technology Letters,* vol. 21, no. 9, pp. 575-577, 2009, doi: 10.1109/LPT.2009.2015058.
[212] Y. Cao, Y. Zhao, Q. Wang, J. Zhang, S. X. Ng, and L. Hanzo, "The Evolution of Quantum Key Distribution Networks: On the Road to the Qinternet," *IEEE Communications Surveys & Tutorials,* vol. 24, no. 2, pp. 839-894, 2022, doi: 10.1109/COMST.2022.3144219.
[213] S. Wang, W. Chen, Z.-Q. Yin, Y. Zhang, T. Zhang, H.-W. Li, F.-X. Xu, Z. Zhou, Y. Yang, D.-J. Huang, L.-J. Zhang, F.-Y. Li, D. Liu, Y.-G. Wang, G.-C. Guo, and Z.-F. Han, "Field test of wavelength-saving quantum key distribution network," *Optics Letters,* vol. 35, no. 14, pp. 2454-2456, 2010, doi: 10.1364/OL.35.002454.
[214] I. Choi, R. J. Young, and P. D. Townsend, "Quantum key distribution on a 10Gb/s WDM-PON," *Optics Express,* vol. 18, no. 9, pp. 9600-9612, 2010, doi: 10.1364/OE.18.009600.
[215] I. Choi, R. J. Young, and P. D. Townsend, "Quantum information to the home," *New Journal of Physics,* vol. 13, no. 063039, 2011, doi: 10.1088/1367-2630/13/6/063039.
[216] E. T. Won, D. Shin, D. Jung, Y. Oh, T. Bae, H. Kwon, C. Cho, J. Son, D. O'Brien, and T. Kang, "Visible light communication: tutorial," *Project: IEEE P,* vol. 802, 2008, doi: IEEE 802.15-<08/0114-02>.
[217] L. U. Khan, "Visible light communication: Applications, architecture, standardization and research challenges," *Digital Communications and Networks,* vol. 3, no. 2, pp. 78-88, 2017, doi: 10.1016/j.dcan.2016.07.004.

[218] T. Gao, L. Rickert, F. Urban, J. Große, N. Srocka, S. Rodt, A. Musiał, K. Żołnacz, P. Mergo, K. Dybka, W. Urbańczyk, G. Sęk, S. Burger, S. Reitzenstein, and T. Heindel, "A quantum key distribution testbed using a plug&play telecom-wavelength single-photon source," *Applied Physics Reviews,* vol. 9, no. 011412, 2022, doi: 10.1063/5.0070966.

[219] P. Ferrand, "Counting photons: from the instruments to the applications " in *presented at the Institut Fresnel, MOSAIC group. Lecture given to the students of the OPSI Master*, ed, 2011.

[220] E. Hecht, *Optics*. Harlow: Pearson Education Limited, 2017.

[221] C. M. Natarajan, M. G. Tanner, and R. H. Hadfield, "Superconducting nanowire single-photon detectors: physics and applications," *Superconductor Science and Technology,* vol. 25, no. 063001, 2012, doi: 10.1088/0953-2048/25/6/063001.

[222] L. You, "Superconducting nanowire single-photon detectors for quantum information," *Nanophotonics,* vol. 9, no. 9, pp. 2673-2692, 2020, doi: 10.1515/nanoph-2020-0186.

[223] A. Huntington, M. Compton, and G. Williams, "Linear-mode single-photon APD detectors," *Optics East,* vol. 6771, 2007, doi: 10.1117/12.751925.

[224] A. Huntington, M. Compton, S. Coykendall, G. Soli, and G. M. Williams, "Linear-mode single-photon-sensitive avalanche photodiodes for GHz-rate near-infrared quantum communications," *MILCOM 2008 - 2008 IEEE Military Communications Conference,* pp. 1-6, 16-19 Nov 2008, doi: 10.1109/MILCOM.2008.4753056.

[225] G. Williams, M. Compton, and A. Huntington, "High-speed photon counting with linear-mode APD receivers," *SPIE Defense, Security, and Sensing,* vol. 7320, 2009, doi: 10.1117/12.817862.

[226] Z. L. Yuan, A. R. Dixon, J. F. Dynes, A. W. Sharpe, and A. J. Shields, "Gigahertz quantum key distribution with InGaAs avalanche photodiodes," *Applied Physics Letters,* vol. 92, no. 20, 2008, doi: 10.1063/1.2931070.

[227] N. Namekata, H. Takesue, T. Honjo, Y. Tokura, and S. Inoue, "High-rate quantum key distribution over 100 km using ultra-low-noise, 2-GHz sinusoidally gated InGaAs/InP avalanche photodiodes," *Optics Express,* vol. 19, no. 11, pp. 10632-10639, 2011, doi: 10.1364/OE.19.010632.

[228] A. Koehler-Sidki, J. F. Dynes, M. Lucamarini, G. L. Roberts, A. W. Sharpe, Z. L. Yuan, and A. J. Shields, "Best-Practice Criteria for Practical Security of Self-Differencing Avalanche Photodiode Detectors in Quantum Key Distribution," *Physical Review Applied,* vol. 9, no. 4, p. 044027, 2018, doi: 10.1103/PhysRevApplied.9.044027.

[229] K. A. Patel, J. F. Dynes, I. Choi, A. W. Sharpe, A. R. Dixon, Z. L. Yuan, R. V. Penty, and A. J. Shields, "Coexistence of High-Bit-Rate Quantum Key Distribution and Data on Optical Fiber," *Physical Review X,* vol. 2, no. 041010, 2012, doi: 10.1103/PhysRevX.2.041010.

[230] J. F. Dynes, W. W. S. Tam, A. Plews, B. Fröhlich, A. W. Sharpe, M. Lucamarini, Z. Yuan, C. Radig, A. Straw, T. Edwards, and A. J. Shields, "Ultra-high bandwidth quantum secured data transmission," *Scientific Reports,* vol. 6, no. 1, p. 35149, 2016, doi: 10.1038/srep35149.

[231] I. Choi, Y. R. Zhou, J. F. Dynes, Z. Yuan, A. Klar, A. Sharpe, A. Plews, M. Lucamarini, C. Radig, J. Neubert, H. Griesser, M. Eiselt, C. Chunnilall, G. Lepert, A. Sinclair, J.-P. Elbers, A. Lord, and A. Shields, "Field trial of a quantum secured 10Gb/s DWDM transmission system over a single installed fiber," *Optics Express,* vol. 22, no. 19, pp. 23121-23128, 2014, doi: 10.1364/OE.22.023121.

[232] S. Cova, M. Ghioni, A. Lacaita, C. Samori, and F. Zappa, "Avalanche photodiodes and quenching circuits for single-photon detection," *Appl. Opt.,* vol. 35, no. 12, pp. 1956-1976, 1996, doi: 10.1364/AO.35.001956.

[233] A. Tosi, A. Dalla Mora, F. Zappa, S. Cova, M. Itzler, and X. Jiang, "InGaAs/InP single-photon avalanche diodes show low dark counts and require moderate cooling," *SPIE OPTO: Integrated Optoelectronic Devices,* vol. 7222, 2009, doi: 10.1117/12.808262.
[234] J. Zhang, M. A. Itzler, H. Zbinden, and J.-W. Pan, "Advances in InGaAs/InP single-photon detector systems for quantum communication," *Light: Science & Applications,* vol. 4, no. 5, 2015, doi: 10.1038/lsa.2015.59.
[235] A. Lord, R. Woodward, S. Murai, H. Sato, J. Dynes, P. Wright, C. White, R. Davey, M. Wilkinson, P. Clinton-Tarestad, I. Hawkins, K. Farrington, and A. Shields, "London Quantum-Secured Metro Network," *Optical Fiber Communication Conference (OFC) 2023,* p. W4K.4, 2023, doi: 10.1364/OFC.2023.W4K.4.
[236] X.-X. Xia, Z. Zhang, H.-B. Xie, X. Yuan, J. Lin, S.-K. Liao, Y. Liu, C.-Z. Peng, Q. Zhang, and J.-W. Pan, "LED-based fiber quantum key distribution: toward low-cost applications," *Photonics Research,* vol. 7, no. 10, pp. 1169-1174, 2019, doi: 10.1364/PRJ.7.001169.
[237] Y. Mao, B.-X. Wang, C. Zhao, G. Wang, R. Wang, H. Wang, F. Zhou, J. Nie, Q. Chen, Y. Zhao, Q. Zhang, J. Zhang, T.-Y. Chen, and J.-W. Pan, "Integrating quantum key distribution with classical communications in backbone fiber network," *Optics Express,* vol. 26, no. 5, pp. 6010-6020, 2018, doi: 10.1364/OE.26.006010.
[238] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, "Overcoming the rate–distance limit of quantum key distribution without quantum repeaters," *Nature,* vol. 557, no. 7705, pp. 400-403, 2018, doi: 10.1038/s41586-018-0066-6.
[239] L. Ma, A. Mink, and X. Tang, "High Speed Quantum Key Distribution Over Optical Fiber Network System," (in eng), *J Res Natl Inst Stand Technol,* vol. 114, no. 3, pp. 149-77, May-Jun 2009, doi: 10.6028/jres.114.010.
[240] A. Biswas, A. Banerji, N. Lal, P. Chandravanshi, R. Kumar, and R. P. Singh, "Quantum key distribution with multiphoton pulses: an advantage," *Optics Continuum,* vol. 1, no. 1, pp. 68-79, 2022, doi: 10.1364/OPTCON.445727.
[241] M. Mirhosseini, O. S. Magaña-Loaiza, M. N. O'Sullivan, B. Rodenburg, M. Malik, M. P. Lavery, M. J. Padgett, D. J. Gauthier, and R. W. Boyd, "High-dimensional quantum cryptography with twisted light," *New Journal of Physics,* vol. 17, no. 3, p. 033033, 2015, doi: 10.1088/1367-2630/17/3/033033.
[242] D. Rogers, J. Bienfang, A. Mink, B. Hershman, A. Nakassis, X. Tang, L. Ma, D. Su, C. Williams, and C. Clark, "Free-space quantum cryptography in the H-alpha Fraunhofer window," *SPIE Optics + Photonics,* vol. 6304, 2006, doi: 10.1117/12.680899.
[243] ID Quantique, "ID Qube Series: NIR," [Online] 2022. [Online]. Available: https://www.becker-hickl.com/wp-content/uploads/2023/02/ID-Qube_Brochure.pdf.
[244] R. Boyd, *Radiometry and the Detection of Optical Radiation*. New York: John Wiley & Sons, Inc., 1983.
[245] Semrock, "Filter Spectra at Non-normal Angles of Incidence," *IDEX Health & Science LLC,* [Online] 2019. [Online]. Available: https://www.idex-hs.com/resources/resources-detail/filter-spectra-at-non-normal-angles-of-incidence#:~:text=As%20the%20angle%20increases%20from,more%20than%20s%2Dpolarized%20light.
[246] Spectrogon, "Narrow Bandpass Filters: Art no: 711M. NB-0655-022," [Online] 2020. [Online]. Available: https://www.spectrogon.com/wp-content/uploads/spectrogon/NB-0655-022-nm.pdf.
[247] Alluxa, "658.7-0.3 OD5 Ultra Narrow Bandpass Filter. SKU: 7308," [Online] 2022. [Online]. Available: https://www.alluxa.com/optical-filter-catalog/ultra-narrow-bandpass/658-7-0-3-od5-ultra-narrow-bandpass/.

[248] Alluxa, "760.7-1 OD4 Ultra Narrow Bandpass Filter. SKU: 7350," [Online] 2022. [Online]. Available: https://www.alluxa.com/optical-filter-catalog/ultra-narrow-bandpass/760-7-1-od4-ultra-narrow-bandpass-filter-25mm/.
[249] O. Elmabrok and M. Razavi, "Wireless quantum key distribution in indoor environments," *JOSA B,* vol. 35, no. 2, pp. 197-207, 2018, doi: 10.1364/JOSAB.35.000197.
[250] O. Elmabrok, M. Ghalaii, and M. Razavi, "Quantum-classical access networks with embedded optical wireless links," *JOSA B,* vol. 35, no. 3, pp. 487-499, 2018, doi: 10.1364/JOSAB.35.000487.
[251] Cree Inc., "BR30 Series LED Reflector Lamp," 2014. Accessed: 3 October 2024. [Online]. Available: https://www.e-conolight.com/media/productdocuments/document/file/BR30%20Series.pdf
[252] T. Komine and M. Nakagawa, "Fundamental analysis for visible-light communication system using LED lights," *IEEE transactions on Consumer Electronics,* vol. 50, no. 1, pp. 100-107, 2004, doi: 10.1109/TCE.2004.1277847.
[253] ASTM G173-03 (2020), "Standard Tables for Reference Solar Spectral Irradiances: Direct Normal and Hemispherical on 37° Tilted Surface," 2020, doi: 10.1520/G0173-03R20.
[254] C. Riordan and R. Hulstron, "What is an air mass 1.5 spectrum? (solar cell performance calculations)," *IEEE Conference on Photovoltaic Specialists,* pp. 1085-1088 vol.2, 21-25 May 1990, doi: 10.1109/PVSC.1990.111784.
[255] D. R. Myers, A. Andreas, T. Stoffel, I. Reda, S. Wilcox, P. Gotseff, B. Kay, and C. Gueymard, *NREL Spectral Standards Development and Broadband Radiometric Calibrations* (Conference: Presented at the National Center for Photovoltaics and Solar Program Review Meeting, 24-26 March 2003, Denver, Colorado.). National Renewable Energy Lab. (NREL), Golden, CO (United States), 2003, pp. Medium: ED; Size: 6 pp. 1-3.
[256] C. A. Gueymard, D. Myers, and K. Emery, "Proposed reference irradiance spectra for solar energy systems testing," *Solar Energy,* vol. 73, no. 6, pp. 443-467, 2002, doi: 10.1016/S0038-092X(03)00005-7.
[257] R. W. Boyd, *Radiometry and the Detection of Optical Radiation*. Wiley, 1983, p. 254.
[258] ID Quantique, "Redefining Measurement. ID120 Visible Single-Photon Detector," [Online] 2021. [Online]. Available: https://www.dyna-sense.com/wp-content/uploads/2020/03/ID120-Datasheet.pdf.
[259] Alluxa, "Alluxa The Next Generation of Optical Filters," [Online] 2017. [Online]. Available: https://www.alluxa.com/optical-filters/ultra-series-thin-films/bandpass-filters/ultra-narrow-bandpass-filters.
[260] Saint-Gobain Glass UK Ltd, "SGG PLANICLEAR. A new standard in clear glass," [Online] pp. 1-4, 14 July 2014. [Online]. Available: https://www.saint-gobain-glass.co.uk/wp-content/uploads/2024/06/PLANICLEAR-2024.pdf.
[261] Shimadzu Corporation, "Solar Transmittance/Solar Reflectance Measurement," [Online] 2022. [Online]. Available: https://www.shimadzu.com/an/service-support/technical-support/technical-information/uv-vis/uv-ap/solar/index.html.
[262] Spectrogon, "Narrow Bandpass Filters: Art No: 713. NB-1370-010," [Online] 2018. [Online]. Available: https://www.spectrogon.com/wp-content/uploads/spectrogon/NB-1370-010-nm.pdf.
[263] International Commission on Illumination (CIE), "Photometry - The CIE System of Physical Photometry," *ISO/CIE 23539:2023 CIE TC 2-93,* 2023, doi: 10.25039/IS0.CIE.23539.2023.
[264] D. Marcuse, "Loss analysis of single-mode fiber splices," *The Bell System Technical Journal,* vol. 56, no. 5, pp. 703-718, 1977, doi: 10.1002/j.1538-7305.1977.tb00534.x.

[265] V. Lee, A. Schreier, G. Faulkner, and D. O'Brien, "Towards the engineering of a quantum key distribution receiver robust to ambient light," *SPIE Photonex,* vol. 12335, 2023, doi: 10.1117/12.2645135.
[266] Analog Devices, "Demo Manual DC499A LTC5100 3.3V, 3.2Gbps VCSEL Driver," pp. 1-8, 2019. [Online]. Available: https://www.analog.com/media/en/dsp-documentation/evaluation-kit-manuals/dc499a.pdf.
[267] Analog Devices, "Demo Manual DC590B USB Serial Controller for Linear Technology QuikEval Demo Boards," pp. 1-10, 2004. [Online]. Available: https://www.analog.com/media/en/technical-documentation/user-guides/dc590bf.pdf.
[268] W. R. Leo, "The NIM Standard," *Techniques for Nuclear and Particle Physics Experiments: A How-to Approach,* pp. 257-261, 1994, doi: 10.1007/978-3-642-57920-2_12.
[269] Meerstetter Engineering, "TEC-1161 TEC Controller Datasheet," pp. 1-8, 2020. [Online]. Available: https://www.meerstetter.ch/customer-center/downloads/category/71-tec-1161-tec-controller-datasheets?srsltid=AfmBOopQBW2WJ7U-ZHMaHmEAcZ6EVQVxGOgVdVCYhu67tq4_qG2qA3xx.
[270] Keysight Technologies, "Agilent 86142B Optical Spectrum Analyzer Technical Overview," pp. 1-10, 2012. [Online]. Available: http://legacy.libertytest.com/assetmanager/uploaded/pdf-20091123-131120-at_86142b.pdf.
[271] Thorlabs, "Tutorial: Principles of Spatial Filters," [Online]. [Online]. Available: https://www.thorlabs.com/newgrouppage9.cfm?objectgroup_id=10768.
[272] L. R. Rabiner and R. W. Schafer, *Theory and Applications of Digital Speech Processing*, 1st ed. Prentice Hall Press, 2010.
[273] ID Quantique, "ID900 Time Controller Series," [Online] pp. 1-4, 2021. [Online]. Available: https://www.dyna-sense.com/wp-content/uploads/2020/03/ID900_Brochure.pdf.
[274] X. Ma, "Unconditional security at a low cost," *Physical Review A,* vol. 74, no. 052325, 2006, doi: 10.1103/PhysRevA.74.052325.
[275] J. Sidhu, T. Brougham, D. McArthur, R. Pousa, and D. K. Oi, "Key generation analysis for satellite quantum key distribution," *SPIE Photonex,* vol. 11881, 2021, doi: 10.1117/12.2599044.
[276] J. S. Sidhu, T. Brougham, D. McArthur, R. G. Pousa, and D. K. L. Oi, "Finite key effects in satellite quantum key distribution," *npj Quantum Information,* vol. 8, no. 1, p. 18, 2022, doi: 10.1038/s41534-022-00525-3.
[277] J. Sidhu, T. Brougham, D. McArthur, R. Pousa, and D. K. Oi, "Satellite quantum key distribution performance analysis and optimization with finite key size constraints," *SPIE Quantum West,* vol. 12446, 2023, doi: 10.1117/12.2651549.
[278] Y. Kaymak, R. Rojas-Cessa, J. Feng, N. Ansari, M. Zhou, and T. Zhang, "A Survey on Acquisition, Tracking, and Pointing Mechanisms for Mobile Free-Space Optical Communications," *IEEE Communications Surveys & Tutorials,* vol. 20, no. 2, pp. 1104-1123, 2018, doi: 10.1109/COMST.2018.2804323.
[279] C. Quintana, H. Chun, R. Mulyawan, G. Faulkner, S. Collins, D. C. O. Brien, E. Xie, J. J. D. McKendry, E. Gu, M. D. Dawson, P. P. Manousiadis, D. A. Vithanage, G. A. Turnbull, and I. D. W. Samuel, "Ultra-wide coverage VLC system with alignment-free receiver," *2018 Global LIFI Congress (GLC),* pp. 1-4, 8-9 Feb 2018, doi: 10.23919/GLC.2018.8319104.
[280] D. Leuenberger, "Optotune mirror presentation. Technology - Products - Applications," [Online] pp. 1-69, August 2021. [Online]. Available: https://www.optotune.com/downloads.

[281] H. Chun, A. Gomez, C. Quintana, W. Zhang, G. Faulkner, and D. O'Brien, "A Wide-Area Coverage 35 Gb/s Visible Light Communications Link for Indoor Wireless Applications," *Scientific Reports,* vol. 9, no. 1, p. 4952, 2019, doi: 10.1038/s41598-019-41397-6.
[282] K. Wang, A. Nirmalathas, C. Lim, and E. Skafidas, "Indoor optical wireless localization system with height estimation for high-speed wireless communications in personal areas," *2012 IEEE International Topical Meeting on Microwave Photonics,* pp. 72-75, 11-14 Sept 2012, doi: 10.1109/MWP.2012.6474057.
[283] M. Medina, D. Kin, A. Shar, Y. Gourman, A. Carmeli, and S. Krylov, "Micro mirrors for MEMS based free space point to point indoor wireless optical network (IWON)," *2015 International Conference on Optical MEMS and Nanophotonics (OMN),* pp. 1-3, 2-5 Aug 2015, doi: 10.1109/OMN.2015.7288893.
[284] Mirrorcle Technologies, "Mirrorcle Technologies MEMS Mirrors - Technical Overview," [Online] pp. 1-7, 2021. [Online]. Available: https://www.mirrorcletech.com/wp/wp-content/uploads/2018/01/Mirrorcle-Technologies-MEMS-Mirrors-Technical-Overview.pdf.
[285] L. J. Hornbeck, "The DMDTM Projection Display Chip: A MEMS-Based Technology," *MRS Bulletin,* vol. 26, no. 4, pp. 325-327, 2001, doi: 10.1557/mrs2001.72.
[286] L. J. Hornbeck, "From cathode rays to digital micromirrors: A history of electronic projection display technology," *Texas Instruments Technical Journal (special DLP issue),* vol. 15, no. 3, pp. 7-46, July-September 1998.
[287] Texas Instruments, "TI DLP LightCrafter 4500 Evaluation Module User's Guide," Manual no. DLPU011F, pp. 1-66, July 2017. [Online]. Available: https://www.ti.com/lit/ug/dlpu011f/dlpu011f.pdf.
[288] P. Gelabert, "A look inside the iView Engine in LightCrafter4500," *Texas Instruments,* [Online] 2013. [Online]. Available: https://e2e.ti.com/support/dlp-products-group/dlp/f/dlp-products-forum/278008/a-look-inside-the-iview-engine-in-lightcrafter4500.
[289] Texas Instruments, "DLP4500 0.45 WXGA DMD," Manual no. DLPS151B, pp. 1-56, May 2022. [Online]. Available: https://www.ti.com/lit/ds/symlink/dlp4500.pdf.
[290] M. Mirhosseini, O. S. Magana-Loaiza, C. Chen, B. Rodenburg, M. Malik, and R. W. Boyd, "Rapid generation of light beams carrying orbital angular momentum," *Optics Express,* vol. 21, no. 25, pp. 30196-30203, 2013, doi: 10.1364/OE.21.030196.
[291] A. D. Rakić, "Algorithm for the determination of intrinsic optical constants of metal films: application to aluminum," *Appl. Opt.,* vol. 34, no. 22, pp. 4755-4767, 1995/08/01 1995, doi: 10.1364/AO.34.004755.
[292] E. Collett, *Field Guide to Polarization*. Bellingham, WA: SPIE Press, 2005.
[293] Thorlabs, "2" Pellicle Beamsplitter, Coated for 45:55 (R:T) Split Ratio for 1-2 um," BP245B3, 2005. [Online]. Available: https://www.thorlabs.com/thorproduct.cfm?partnumber=BP245B3.
[294] Texas Instruments, "DLP4500NIR 0.45 WXGA Near-Infrared DMD," Manual no. DLPS147B, pp. 1-48, May 2022. [Online]. Available: https://www.ti.com/lit/ds/symlink/dlp4500nir.pdf?ts=1739205312331&ref_url=https%253A%252F%252Fwww.ti.com%252Fproduct%252FDLP4500NIR.
[295] Texas Instruments, "DLP471TP 0.47 4K UHD DMD," Manual no. DLPS173B, pp. 1-48, July 2023. [Online]. Available: https://www.ti.com/lit/ds/symlink/dlp471tp.pdf?ts=1739215518679&ref_url=https%253A%252F%252Fwww.ti.com%252Fproduct%252FDLP471TP.
[296] Texas Instruments, "DLP9500 DLP 0.95 1080p 2x LVDS Type A DMD," Manual no. DLPS025F, pp. 1-56, July 2023. [Online]. Available: https://www.ti.com/lit/ds/symlink/dlp9500.pdf?ts=1739212800281.

[297] SORAA, "SORAA Vivid MR16 Constant Current (SM16C-CC1-10D-927-03)," [Online] 2020. [Online]. Available: https://www.soraa.com/assets/cloud/product_specs/mr16-constant-current/01359/spec_sheet.pdf.
[298] L. Hornbeck, "Digital Light Processing for high-brightness high-resolution applications," *Electronic Imaging '97,* vol. 3013, 1997, doi: 10.1117/12.273880.