Wavelength Selection for Satellite Quantum Key Distribution

Shane Hearne

Walton Institute
South East Technological University

Supervisor: Dr Deirdre Kilbane

MSc. Thesis by Research.
Submitted in fulfilment of the requirements
for the degree of MSc in Quantum Satellite Communications
at South East Technological University, February, 2023.

SE
TU
Ollscoil
Teicneolaíochta
an Oirdheiscirt
South East
Technological
University

I hereby certify that this material, which I now submit for assessment on the programme of study leading to the award of MSc in Quantum Satellite Communications is entirely my own work and has not been taken from the work of others save and to the extent that such work has been cited and acknowledged within the text of my work.

Signed: Shane Hearne ID No: 20075826

Date: 25/02/23

Abstract

While the advancement of quantum computers threatens the security of current encryption methods, the satellite Quantum Key Distribution (QKD) channel is expected to enable global quantum communications. However, the availability of these systems is limited by background noise due to solar radiation and strong attenuation caused by turbulence and other adverse weather conditions. This work combines filtering techniques, adaptive optics, and optimal wavelength selection to permit daytime QKD through realistic atmospheric conditions. The secret key rate is determined using the decoy-state BB84-QKD protocol and used as a performance metric to investigate the performance of wavelengths ranging from the visible and near-infrared regions to the short-wave, mid-wave, and long-wave infrared regions of the electromagnetic spectrum. The satellite downlink channel is modelled to determine the signal gain accounting for diffraction-induced beam spread, extinction loss and turbulence-induced wavefront distortions while the background probability is calculated as a function of spectral radiance. Secret key rate optimization is a multivariate problem so a wavelength comparison cannot be done in isolation but instead requires a number of other parameters to be varied simultaneously. To this end, the secret key rate is determined for a range of wavelengths, receiver sizes and initial beam waists to reveal what combination achieves the best performance through a variety of atmospheric conditions. Additionally, satellite communications place physical limitations on transmitter and receiver sizes so the optimal wavelengths and secret key rates are determined for a number of incremental component size constraints.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

The following thesis is organised into 5 chapters. Chapter 1 begins by exploring a brief history and background of quantum key distribution (QKD), to help clarify the motivations of this research. Chapter 2 describes the methodologies used to compile this thesis. Chapter 3 provides a breakdown of relevant theory for the protocols and mathematical models used throughout this work. In chapter 4, these models are used to simulate the satellite-earth downlink channel and compare the performance of different wavelengths in a variety of atmospheric conditions, followed by a detailed analysis and discussion. Finally, chapter 5 concludes this thesis by summarising the results and suggesting some avenues for continued work on this topic.

1.1 Cryptography

The first transistor was successfully demonstrated in 1947 and ever since the rapid growth of semiconductor technology has accelerated the digitalization of society. With each passing year, the integrity of modern life increasingly relies on secure communications. While secure communication is not exclusive to the modern age, its importance has never been so universal. Cryptography is the study of secure communications techniques, that allow participants to share private data amongst themselves, where only the intended recipient is able to view the contents of that data. The most common type of cryptographic scheme used today is public-key cryptography [1]. In public-key cryptography, the key has two parts: public and private. Data encrypted with the public key can only be decrypted with the private key, and data encrypted with the private key can only be decrypted with the public key. The security of public-key cryptography is predicated on the unproven premise that certain problems are difficult to solve, such as integer factorization and the discrete logarithm problem. As a result, the system could be sensitive to advances in computational power or the development of more efficient algorithms. Indeed, utilizing quantum computers, there is already an algorithm that can theoretically be used to solve these problems in polynomial time [2]. This means that someone with access to a fault-tolerant quantum computer could theoretically break the encryption and access secure data. This algorithm is called Shor's algorithm and was developed in 1994 [3] by Peter Shor to allow a quantum computer to efficiently factor a large integer into its primes, exponentially faster than a classical computer ever could. His discovery sparked an explosion of interest in the fields of quantum information, communication and computation [4]. Seven years later, Shor's algorithm was demonstrated during a real quantum computing experiment in 2001. In this experiment, IBM researchers used seven spin $-\frac{1}{2}$ nuclei in a molecule as qubits and manipulated them using nuclear magnetic resonance techniques [5]. They used Shor's algorithm to factorise 15 into its prime factors, 5 and 3. This verified that Shor's algorithm does work for factorisation and could potentially be used to break encryption. However, quantum computers are still in their infancy and have a long way to go before they can break current encryption methods. This gives researchers some time to begin looking at ways to establish provably secure communications.

1.2 Quantum Cryptography

Two possible methods have emerged:

1. Post-quantum cryptography which looks for alternative computationally intense mathematical problems that can't be broken by quantum algorithms

2. Quantum key distribution, which in contrast to classical cryptography, uses the principles of quantum mechanics to provide an unconditionally secure way to share encryption keys

The concept of quantum key distribution (QKD) was first proposed in the 1970's and is now perhaps the most mature quantum technology, being commercially available for over 17 years. QKD is a set of techniques that utilize the laws of quantum mechanics such as the Heisenberg uncertainty principal or entanglement, to distribute encryption keys. These protocols can even detect the presence of an eavesdropper in the system who is attempting to intercept the key. In 1984, Bennett and Brassard [6] gave the first description of a quantum key distribution protocol, the BB84 protocol, which remains one of the most relevant quantum algorithms today. Its security is based on the no-cloning theorem [7] which follows from the Heisenberg uncertainty principal, making the protocol provably secure provided the existence of an authenticated classical channel [8]. Thus the BB84 protocol allows two parties, Alice and Bob, to establish secure communications by allowing them to detect the presence of an eavesdropper, Eve. A detailed deception of this protocol and the associated quantum properties is given in chapter 2.

The following years saw the development of numerous novel QKD schemes [9, 10, 11, 12, 13]. The E91 protocol described by Artur Ekert in 1991 uses a single-photon source to generate entangled pairs of photons, and sends them to Alice and Bob. When Alice and Bob measure the quantum states, they will get associated results for each measurement that they chose the same basis for and after eliminating the photons recorded on different bases, they will have a string of bits correlated to each other. Finally they can test Bell's Inequality to check for the presence of Eve [9]. This was the first proposal of a completely new class QKD schemes, Entanglement-Based schemes. In the following year Bennett and Brassard et al proposed their own Entanglement-Based protocol BBM92 [10]. Now there were two types of QKD schemes, Entanglement-Based (EB) schemes in contrast to the original Prepare and Measure (PM) schemes. Some other Prepare and Measure schemes that followed include Bennett's 1992 protocol B92 [11] and the Six State protocol SSP in 1998 [12].

Most of the DV-QKD protocols are ideally implemented using single-photon sources but attenuated laser pulses (weak coherent states) are commonly used in real-world QKD systems, and they occasionally emit more than one photon. This makes the system vulnerable to sophisticated eavesdropping attacks [14, 15, 16]. As a result, new QKD protocols, such as the decoy-state QKD protocol [17] and the measurement-device independent QKD (MDI-QKD) protocol [18][19], have been developed to defend QKD systems from such flaws. A detailed description of the decoy-state QKD protocol is given in chapter 3. A summary of some of the most relevant QKD protocols is given in Table 1.1

Every protocol mentioned thus far falls under the family of Discrete-Variable (DV) QKD protocols. They all use either the polarization or phase of photons to encode the bits and establish secret keys between Alice and Bob. These protocols focus on and require single-photon sources and detectors. However, in 1999 Ralph proposed an alternative approach [13] that used standard telecommunication devices to transmit and detect quantum states. This new family became known as Continuous-Variable (CV) QKD, which uniquely encodes information into the quadratures of randomly selected coherent states and uses efficient and cost-effective homodyne or heterodyne detection. However, there are still substantial obstacles to overcome, such as the necessity to reduce classical communication between Alice and Bob during key generation [20].

Table 1.1: Summary of Quantum Key Distribution protocols reviewed

QKD Protocol	Description	Year	Authors
BB84	A widely used QKD protocol that utilizes a quantum channel to securely exchange encoded qubits between a sender and a receiver. It employs two orthogonal bases, such as rectilinear and diagonal, for qubit encoding. By exchanging and comparing measurement basis information, the protocol allows for the detection of potential eavesdropping attempts, ensuring secure key distribution between the communicating parties.	1984	Charles Bennett, Gilles Brassard [6]
E91	Utilises entanglement to establish secure key distribution. It uses pairs of entangled particles shared between the sender and receiver, and measurements on these particles generate a shared secret key.	1991	Artur Ekert [9]
B92	A simplified version of BB84 that reduces the number of possible states.	1992	Charles Bennett [11]
BBM92	An entanglement-based protocol that combines elements of the BB84 and B92 protocols. It uses entangled pairs of particles to distribute secret keys, reducing vulnerability to certain types of eavesdropping attacks.	1992	Charles Bennett, Gilles Brassard, N. David Mermin [10]
Six State	Uses six non-orthogonal states for encoding qubits, allowing for higher key generation rates compared to BB84. It incorporates phase encoding and randomness in the measurement basis to improve security.	1998	Dagmar Bruss [12]
Decoy-State	Enables secure key distribution even in the presence of high optical losses, making it suitable for long-distance communication scenarios. It employs decoy state techniques to estimate the channel loss and adapt the encoding scheme accordingly, ensuring reliable key distribution over long distances.	2003	Won-Young Hwang [17]
CV-QKD	Utilizes the phase properties of coherent light to establish secure key distribution. It leverages a reference pulse to encode information in the phase of the signal pulse, providing resistance against certain types of eavesdropping attacks.	2000	Timothy C Ralph [13]
MDI-QKD	Ensures resistance against attacks on the measurement devices used by implementing a special measurement technique known as Bell-State measurement between the sender and receiver. This allows for the generation of secure keys even when the devices are untrusted, making MDI-QKD a robust solution for secure quantum communication.	2012	Lo, Hoi-Kwong and Curty, Marcos and Qi, Bing [18]

1.3 Quantum Channels

The fundamental concept of classical information and classical computation is the bit, which is simply a two state system where the two states are referred to as 0 and 1 [21]. All classical information can be represented by grouping together these bits and any arbitrary computation is derived by the manipulation of these bits. Quantum information theory is built upon its own analogous concept, a basic element called the quantum bit, also known as a qubit [4]. A qubit is a quantum system with two orthonormal basis states $|0\rangle \, and \, |1\rangle$ which is represented using Dirac notation [4].

There are a variety of possible physical implementations of a qubit, such as the polarization states of photons, the spin states of electrons or the charge state of quantum dots [22]. While it is still too early to determine which paradigm will dominate quantum computing, almost all quantum key distribution protocols are designed using photons as qubits. Photonic QKD benefits from a huge selection of advanced components thanks to widespread use in the classical telecommunications industry allowing quantum researchers to utilize advanced communication infrastructure. The most common classical communication channel is optical fibre, which can efficiently carry information around the globe, using amplifiers to boost the signal as it travels. However, in quantum communication, the no-cloning theorem prevents the use of amplifiers, and so the probability that the qubit gets absorbed or depolarised grows exponentially with the length of the fibre [23]. There are two viable solutions to this problem, quantum repeaters and free-space optical communication (FSOC). Quantum repeaters work by dividing the communication distance into smaller regions where keys are separately distributed to each region, followed by entanglement exchange and a purification process that links together adjacent nodes [24]. The practical implementation of these repeaters requires a quantum memory which remains a challenge.

In the absence of quantum repeaters, research in fibre quantum key distribution focuses on extending the maximum distance and integrating quantum signals with the existing classical networks. While early QKD demonstrations used separate dark fibres, for real-world applications it makes much more sense to build QKD into preexisting infrastructure. However, this comes with a number of challenges, such as the weak strength of the quantum signals relative to the classical signals and the much shorter transmission distance [25]. Additionally, any interaction between quantum and classical pulses has the potential to degrade the quality of quantum signals and affect quantum states. Despite these limitations, there are already a number of quantum networks established across the globe. The Defense Advanced Research Project Agency (DARPA) quantum network was set up in the USA [26], the Secure Communication based on Quantum Cryptography (SECOQC) project in Europe [27], the Cambridge quantum network in the UK [28] and a project connecting 4 cities in China [29], to name a few. However, most of the early long-range experiments and networks relied on trusted repeater nodes (TRN) to overcome the short quantum signal transmission distance. Some recent works have attempted to remove TRN's using measurement-device independent (MDI) QKD [19] and twin-field (TF) QKD [30]. In a 2021 paper [31], the authors publish the results of a successful 511 km link between two cities, using Twin-field QKD. In 2022, an experimental QKD system demonstrated a secure distance of 833.8 km while tolerating a channel loss greater than 140 dB [32].

An alternative solution would be to use FSOC to establish a satellite-earth link as demonstrated by the Micius satellite [33, 34], which successfully distributed keys over a distance of 1200 km. Indeed the satellite FSOC channel has been the subject of numerous research papers [35, 36, 37, 38, 39]. In the absence of quantum repeaters, quantum satellite communications are seen as essential infrastructure for achieving long-range quantum communication and establishing a global quantum internet. Additionally, quantum states can be transmitted across much longer distances using free-space optical satellite communication than is possible with repeater-less fibre communication. This is because the amount of secret bits that can be distributed across a communication channel is limited by that channel's transmissivity η, and cannot exceed its secret key capacity $-log2(1-\eta)$ bits/use [40]. This has become known as the Pirandola-Laurenza-Ottaviani-Banchi (PLOB) bound [41]. Thus the communication rate of a repeater-less fibre channel is fundamentally limited due to exponential decay in transmissivity with distance. In contrast, the satellite channel experiences far less loss. The signal can be approximated by a Gaussian beam which if travelling in a vacuum, is limited only by diffraction of the beam and the limited size of the receiver. However, the satellite-earth channel is not a vacuum and the channel is subject to a range of detrimental effects. In addition to diffraction-induced loss, the beam is degraded by the atmospheric effects such as to absorption, scattering and turbulence. One of the biggest limiting factors is background noise caused by solar radiation which makes day-time operation very difficult [42, 43, 44].

For most QKD links, the satellite is a trusted-node that performs QKD operations with various ground stations in order to establish separate secret keys with each. All keys are kept by the satellite, while the stations only have access to their own. To establish a secret key between any two ground stations, the satellite combines their respective keys and broadcasts their bit-wise parity. Using this parity, the individual ground stations can retrieve each other's keys. Because the original keys are separate secret strings, their bit-wise parity is merely a uniformly random string, hence the parity announcement gives potential eavesdroppers no relevant information. The security of this system requires that the satellite must be trusted because access to the data gathered by the satellite would provide an eavesdropper with complete knowledge of the key [42].

There are two types of quantum satellite communication links, uplinks, in which the ground station sends signals to a receiver in space, and downlinks, in which the satellite delivers signals to the ground. Each configuration has advantages and disadvantages, but downlinks are the most widely recommended scenario for practical QKD and the only one that has been implemented so far. This is largely due to lower losses associated with downlink channels, namely the reduced effect of turbulence. The effects of turbulence on a propagating beam will differ significantly between uplink and downlink due to interactions between the beam spot size and the size of the turbulent eddies. Most turbulent effects occur within the lower 20 km of the atmosphere, so the uplink beam encounters turbulence when its waist is still small and susceptible to beam wander and beam spread. In the downlink, the beam travels hundreds of kilometres before it interacts with significant turbulence, at which point the beam waist is large and more resilient against both beam wander and beam spread [40]. A benefit to using the uplink channel is that it eliminates the need to operate a single-photon source on-board the satellite, instead only requiring the installation of a receiver.

The three main categories of satellite orbital altitudes are Low Earth orbit (LEO), Medium Earth orbit (MEO), and Geostationary orbit (GEO). LEO's are located between 160 km and 3000 km in altitude (typically below 900 km), GEO has a height of 35,786 km, while MEO corresponds to all orbits between LEO and GEO [42]. LEO and GEO are the two most viable solutions for satellite QKD applications. LEO satellites benefit from their proximity to the ground, which decreases diffraction-induced losses. However, their rapid speed relative to the Earth's surface makes accurate pointing during signal transmission difficult, while the satellite flyover period is limited. In contrast, the high altitude GEO satellites are at rest relative to the Earth's surface but at the expense of lower channel efficiency. All current QKD satellites orbit at LEO altitudes to decrease transmission loss but this significantly limits the availability of that system. For example, the Micius satellite is on a 500 km sun synchronous orbit, passing over the Xinglong ground station for 5 minutes every night at roughly 00:50 hours local time [38]. So while there are advantages to using satellite QKD over fibre QKD, there is still a long way to go before either technology can provide global coverage.

1.4 Wavelengths for Satellite QKD

Emerging from the International Commission on Illumination, optical radiation has been classified into three categories IR-A (700–1400 nm), IR-B (1400–3000 nm), and IR-C (3000 nm–1 mm) which are commonly sub-classified into [45]:

- Near-infrared (NIR) 750 nm - 1.4 μm
- Short-wavelength infrared (SWIR) 1.4 - 3 μm
- Mid-wavelength infrared (MWIR) 3 - 8 μm
- Long-wavelength infrared (LWIR) 8 - 15 μm
- Far-infrared (FIR) 15 μm - 1 mm

In addition, another option for FSO and QKD systems is the mostly transparent visible window ranging from 400 - 700 nm.

1.4.1 Commonly Used Atmospheric Windows

Near-Infrared:
The low attenuation NIR window is supported by high performance, cost-effective optical sources and detectors readily available from the semiconductor industry. 780 nm one of the most commonly used channels for both FSOC and QKD [46, 47, 48] and wavelengths across the whole NIR window have seen widespread use. The major drawback of using this window for laser communication is the limited power imposed by eye safety regulations. This limitation applies to wavelengths between 400 nm and 1400 nm due to the transparency of vitreous fluid in the eye. While a higher power system doesn't directly affect the performance of the QKD protocol, it could help transmission through unfavourable atmospheric conditions.

Short-Wavelength-Infrared:
The SWIR window is probably the most commonly used region for both FSO and QKD, specifically the channel around 1.55 μm has been studied extensively in the literature [49, 50, 51] due to the maturity of optical components with widespread use in the telecommunications industry. Additionally, there is a significant dip in spectral radiance relative to the visible and NIR wavelengths. Systems operating at in the SWIR window benefit from high transmission, low radiance and can safely transmit approximately 100 times more power than equivalent systems operating at 780nm [47].

Visible:
The authors in [52] show that the use of adaptive optics combined with tight filtering can enable sufficiently high secret key rates (SKR) using visible wavelengths in a satellite downlink channel, in particular they utilize a dip in spectral radiance near 431 nm. Because the beam spot size is proportional to the wavelength, using smaller wavelengths allows even tighter spatial filtering resulting in a higher signal to noise ratio. Filtering becomes even more important in conditions of low visibility, where transmittance decreases while spectral radiance tends to increase due to additional atmospheric scattering.

1.4.2 Infrared free-space Optical Communications

Most FSOC and QKD systems operate using wavelengths in the near-infrared (NIR) or short-wavelength infrared (SWIR) due to the abundance of optical components at those wavelengths and the overlap with the telecommunication and semiconductor industries [38, 53, 54]. However, limited availability due to adverse atmospheric conditions and high background noise has motivated researchers to look at alternative wavelengths [55, 56, 57]. Although the benefits of longer wave FSOC systems are still being debated, some papers have pointed to the potential improvements in propagation through fog and turbulence [58, 59]. In this section, some of the research regarding wavelength selection for satellite free-space optical communication and quantum key distribution is presented. Specifically a literature review is undertaken, focusing on MWIR and LWIR FSO and QKD systems.

Adaptation of telecommunications components in the NIR and SWIR spectral regions has been the foundation of most commercially available FSOC systems. In contrast to fibre-based channels, the FSOC atmospheric channel has distinct properties that must be considered. Molecular absorption, light scattering from aerosols, rain, fog and even snow all make free-space optical propagation a more complex and less controllable channel. As a result, the choice of source wavelength is an important component in the design of these systems, and it is critical to investigate whether using longer wavelength systems can provide a considerable advantage. Historically, long-wavelength laser systems lacked the advantages of typical semiconductor telecommunication devices, such as small size, high bandwidth and high quantum efficiency, which deterred researchers from exploring the capabilities of longer wavelength FSOC and QKD systems. However, advancements in quantum cascade laser technology have enabled researchers to begin investigating the potential advantages of longer wave FSOC and QKD [60, 61, 62, 63]. Quantum cascade laser technology has advanced to the stage where an efficient, high power beam can be produced from 3.4 μm to 16 μm and operated at room temperature [64].

A 2002 paper used quantum cascade laser technology [61] to see how a longer wavelength would affect the link's quality and stability. Their wavelength of choice was 8.1 μm and they found that there were no variations in sensitivity for common weather situations such as sunshine, heavy rain, and thunderstorms. However, in deep fog when visibility is close to zero, the researchers observed a significant variation in the performance of the 8.1 μm link relative to the near-infrared link. As the fog was decreasing, the LWIR link regained nearly 70% of its clear sky transmission while the NIR link was still below the detection limit. The following year, researchers set out to analyze the performance of a short range terrestrial link as a function of wavelength [65]. Considering wavelengths ranging from 400 nm to 20 μm operating in a range of different weather conditions, they conclude that for all cases examined, the 9–13 µm band was preferred with the best transmissivity towards 11 μm. In the same year, Maha Achour published a paper defending her claim that 10 μm has the best free optical performance [66]. Through numerical modelling she showed that long-wavelengths have better fog penetration than shorter wavelengths, up to double the transmission for stable fogs and ten times for selective fogs. Additionally, she argues that components with appropriate performance levels already exist to construct commercially viable 10 μm FSO devices.

Further experimental investigations of long-wave propagation were conducted by Colvero et al in 2005 [62] and 2007 [67]. They compared the performance of 800 nm, 1600 nm, 10 μm in the 2005 experiments and 780 nm, 850 nm, 9.1 μm in a 2007 follow up experiment. Between the experiments, they covered a wide range of atmospheric conditions and weather effects. In all cases, the 9.1 μm and 10 μm LWIR wavelengths outperformed the NIR and SWIR wavelengths. In a 2012 paper, a group of researchers review the use cases for each wavelength region [68]. NIR wavelengths are mostly used for semiconductor laser technology, the 1550 nm SWIR channel is the dominant spectral region for long-distance telecommunications, MWIR wavelengths are used for missile guidance and LWIR is used for thermal imaging. So far, it is clear that the LWIR offers the best performance through a wide range of conditions yet no practical FSO systems utilize these benefits. Note that all experiments mentioned so far refer to terrestrial propagation and the benefits of LWIR satellites links had yet to be determined.

The motivations of a 2016 paper [69] were to predict terahertz attenuation under pristine conditions. As part of this study, they compare the performance of three simulation software packages, namely HITRAN on the Web (HotW), MODTRAN and LBLRTM. HITRAN on the Web uses high resolution spectral line-by-line methods which access the HITRAN (the HIgh-resolution TRANsmission) molecular spectroscopic database [70] and can be used to calculate the spectral attenuation. MODTRAN adopts a spectral band method, which generates mean band transmittance approximations based on the underlying spectroscopy [71] extracted from the HITRAN database. Finally, the spectral resolution advantage of 'HITRAN on the Web' is combined with the accurate broader spectral features of MODTRAN in LBLRTM (Line-By-Line Radiative Transfer Model). LBLRTM queries the HITRAN database to extract gaseous absorption line parameters and calculates spectral transmittance [72] using a line-by-line approach. The authors find the line-by-line algorithm used by LBLRTM to be the most accurate model but it is worth noting that in their comparison they use MODTRAN 4 and since the release of their paper, both MODTRAN 5 and 6 have been released, with MODTRAN 6 introducing its own line-line algorithm [73]. The LBLRTM algorithm is used to calculate the transmission for an earth-satellite link with the ground receiver located at Giza [69]. The satellite is at a zenith angle of 33 degrees and their results are presented in Figure 1.1 where some transmission windows are easily identified. The authors acknowledge the presence of three such windows with cut off transmittance of 50%, the first from 22.6 THz to 38.2 THz, another at 59.1 THz to 65.9 THz and a final starting at 72.4 THz and ending at 90.0 THz. In addition to transmittance, the Planck spectrum is plotted for a black-body radiator at 296 k to represent the solar radiation emitted from earth. This radiation peaks at a frequency of 30.6 Thz which is equivalent to a wavelength of 9.8 μm. Interestingly the authors do not include a similar Planck spectrum plot for a black-body equivalent to the sun. A block-body radiator with a temperature of 5800 K would have a peak in radiation at approximately 500 nm. The radiation that reaches the receiver will be a combination of both solar and terrestrial radiation so it is important to consider both phenomena. Another important note is that the transmittance values are highly dependent on zenith angle (the angle between the satellite and the zenith, see Figure 1.2), and lower zenith angles will have significantly better transmittance than higher zenith angles due to a reduced atmospheric propagation path. While there is some transmission data in the literature,

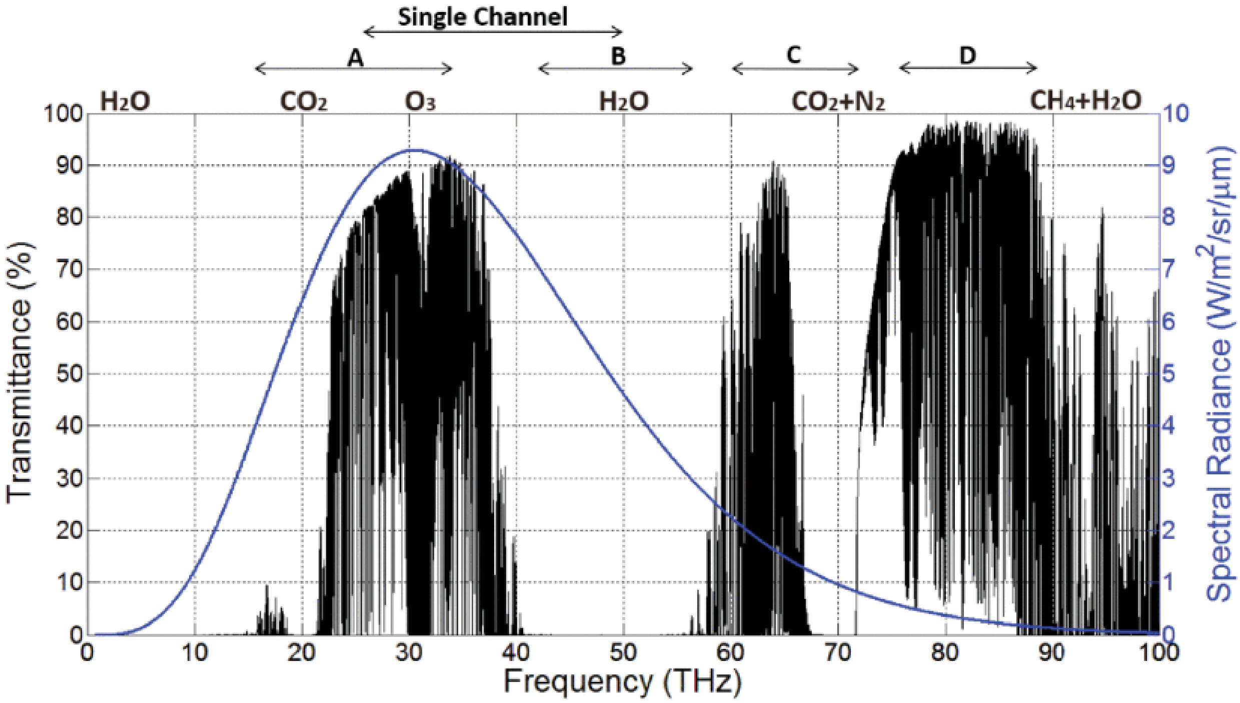


Figure 1.1: LBLRTM transmittance for a ground receiver located at Giza with a 33 zenith angle shown in black with the black-body spectrum at 296 K as a function of wavelength overlaid in blue [69]

access to spectral attenuation software like those described above, is essential to adequately model the satellite channel.

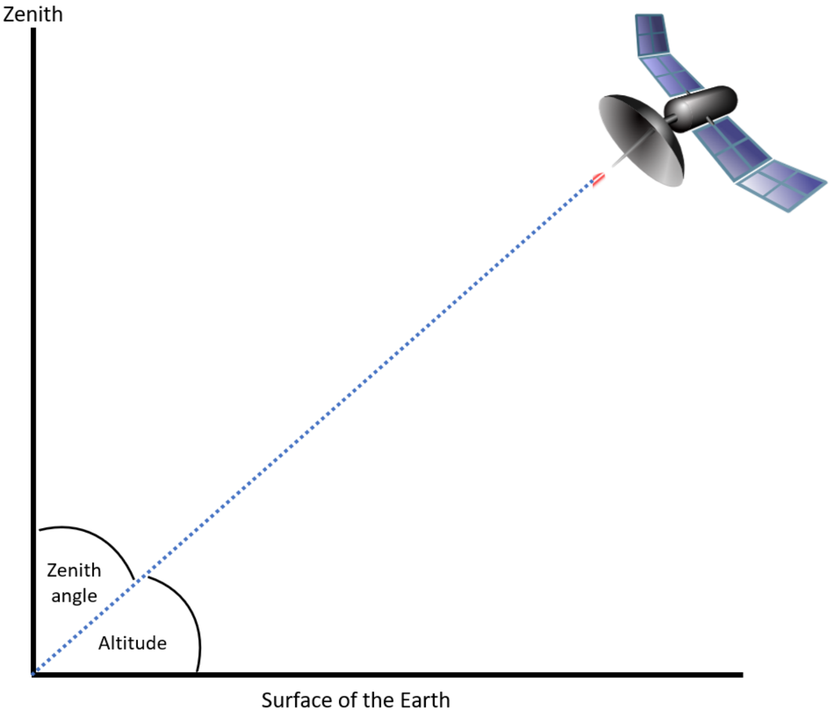


Figure 1.2: Schematic depicting the zenith angle and the altitude angle.

More recent studies into long-wave FSOC include a 2019 paper which reviews MWIR and

LWIR technology and develops a suite of simulation tools to demonstrate the advantage of LWIR propagation through turbulence [74]. Through development of a 10.6 μm FSOC test bed, they demonstrate the feasibly of building high performance MWIR and LWIR FSO systems. In the same year, the performance of a MWIR link is directly compared to a SWIR link in the presence of low visibility conditions [75]. Their results show how the 4 μm MWIR wavelength can achieve the same link performance as the 1.55 μm SWIR wavelength, while operating with at 33 % reduction in visibility. Even more recently, two papers were published in 2021, a quantum cascade laser review paper [63] which evaluates the MWIR region for use in wireless communication systems and investigates the transmission rate of such a system, and a paper published at the end of the year which demonstrates a 10 Gbit per second data rate using a 9 μm free-space optical system. Their research utilizes state of the art technology including a quantum cascade laser and a quantum cascade detector. Furthermore, as the predicted bandwidth is in the 50–100 GHz range, Terabit per second data rates should be achievable making this technology a feasible solution for 6G communications [76].

To conclude this section, while NIR and SWIR wavelengths have typically been used in free-space optical communications due to the maturity of optical components, wavelengths in MWIR and LWIR windows remain largely unexplored for both FSOC and QKD due to a historical lack in high performance devices operating at these wavelengths. However, there is a growing interest in longer wavelength communication fueled by the development of long-wave technology and driven by superior propagating in adverse weather conditions.

1.4.3 Quantum Key Distribution

Despite the interest in long-wavelength classical communications, there are very few studies which attempt to utilize the benefits of the MWIR or LWIR for quantum communication. One of the earliest attempts was in a 2008 paper [77], where the focus of their study was to investigate the feasibility of MWIR QKD. They use the BB84 QKD protocol, which is a Discrete Variable (DV) protocol and requires single-photon sources and detectors. In 2008 there were no single-photon sources operating at their chosen 4.65 μm wavelength so they utilized frequency up-conversion and Sum Frequency Generation (SFG) to convert infrared photons to visible photons which were measured on a Silicon Avalanche Photodiode (Si APD). However, this process generates a lot of noise which ultimately degrades the performance of the system below that of an equivalent system operating at 780 nm. Even while SFG with strong pump powers can improve the single-photon detection efficiency at this wavelength, the noise rate is largely exacerbated by background radiation from up-converted thermal photons, resulting in a limited loss budget. As a result, under clear weather conditions the system using SFG at 4.6 μm would be poor in comparison to typical systems. Despite this additional noise, the 4.6 μm system still out performed the 780 nm system in conditions of low visibility.

In a paper titled 'Quantum Cryptography Approaching the Classical Limit' [78], the authors examine the security of Continuous-Variable (CV) quantum cryptography as the sender station's unknown preparatory noise increases significantly. They demonstrate that as long as channel transmission losses do not exceed 50%, security is not dependent on channel transmission and is hence extremely resistant to significant quantities of extra preparation noise. This allowed them to consider longer wavelengths than those typically used and they discovered that zones of security exist all along the infrared spectrum, even into the microwave region. The key takeaway is that at room temperature, CV-QKD running at lower frequencies (longer wavelengths) introduces a large quantity of thermal noise. For direct reconciliation in the MWIR range, transmission greater than 80% is necessary. They note that CV-QKD is still theoretically achievable across short distances in the infrared and microwave regimes.

In a 2018 experiment [79], researchers test the feasibility of continuous-variable wireless quantum key distribution (WQKD) in the terahertz (THz) band with thermal Gaussian states. They investigate indoor continuous-variable QKD by varying the frequency from 0.1 - 1 THz and find that free-space loss is the primary limiting factor on the secure transmission distance for cases of low gain and uncover a direct relationship between antenna diameter and maximum security distance.

Source and detector limitations are not the only reason that researchers have primarily focused on shorter wavelengths. In the satellite downlink channel, diffraction of the beam is the primary loss factor and also plays a major role in uplink loss. In [57], the authors address the feasibility of inter-satellite continuous-variable quantum key distribution at terahertz frequencies. In that paper, they focus on communication between satellites and can ignore the effects of the atmosphere, thus they employ a diffraction only model. Diffraction-losses are proportional to the square of the wavelength so the efficiency of their model decreases with increasing wavelengths. This observation had discouraged previous researchers from using longer wavelengths for quantum satellite communications. However, the results of the paper conclude that THz frequencies can be used for inter-satellite QKD. They also determine what conditions must be met for a purely diffracting beam propagating over 500 km to produce non-zero QKD rates [57]. They find that frequencies as low as 30 THz are practical even with low detection efficiencies. However, their results show that performance tends to increase with higher frequencies (shorter wavelengths) and lower temperatures. It is worth noting that this research was undertaken with micro-satellites in mind and that lower frequencies (longer wavelengths) require larger optical components due to the increase in diffraction-induced beam spread. Furthermore, this work does not consider any of the proposed advantages of using longer wavelengths such as propagation through adverse weather conditions or reduced solar radiance. However, they do show that terahertz quantum entanglement distribution and terahertz quantum key distribution are realistic microsatellite deployment alternatives. The authors conclude that a lower temperature lowers the available frequency, as does a good channel with a higher transmissivity.

A recent 2020 study titled 'Terahertz Quantum Cryptography' [80], aims to determine the feasibility of THz quantum cryptography in the context of continuous-variable quantum key distribution. In summary they find that thermal noise is the most detrimental factor below 1 terahertz, while atmospheric absorption is the most detrimental factor at higher frequencies. Direct reconciliation is confined to high-transmission situations, owing to poor detector efficiencies of 10%. Reverse reconciliation on the other hand, is less influenced by poor detector efficiency and a positive key can be obtained with a transmissivity as low as 10 %. In conclusion, high data rate THz QKD is possible over short distances but not suitable for long-range communication, achieving roughly 220 m using reverse reconciliation. The authors note that this is mostly a limitation imposed by atmospheric absorption. Although looking at Figure 1.1, its not clear why there was such a reduction in performance relative to other wavelengths. This may be due to the fact that Figure 1.1 depicts the transmission for a dry location under pristine conditions. It is important to note that terahertz are heavily absorbed by water vapour and as such, the desert condition may be misleading. Additionally, most of the water vapour is in the lower atmosphere, making terrestrial propagation more difficult, especially at terahertz frequencies.

Since the 2008 paper [77] using SFG to convert MWIR photons to visible for detection, almost all QKD research using MWIR wavelengths has been focused on continuous-variable QKD. This is understandable as MWIR wavelengths combined with the SFG method are demonstrably worse than using standard wavelengths, at least in clear conditions. As implementation of continuous-variable QKD protocols does not require single-photon sources or detectors, it makes sense to extend it to longer wavelengths, where lack of such components has limited research in long-wave discrete variable QKD. However, longer wave CV communications are limited by the preparation noise incurred when encoding the quantum state with information which limits the distance of quantum cryptography. To bring about the next communication revolution, new devices must be developed. The advancement of quantum cascade lasers has already been discussed and they are now at a point where they can be used as an effective source for QKD. Recent breakthroughs in superconducting sensor technology are enabling highly efficient single-photon detection for much of the electromagnetic spectrum [81, 82, 83]. Although superconducting nanowire single-photon detector (SNSPD) technology is relatively new and there is still much work to be done to build commercial devices with high efficiency in the MWIR and LWIR, the proof of principle demonstrations in [82] show promising stability and efficiency. From low-frequency microwave wavelengths to high-frequency optical wavelengths, several superconducting sensors and detectors have exhibited unrivalled performance across practically the entire electromagnetic spectrum. It is clear that as long as QKD systems use photons as quantum, these detectors will play an indispensable role for the future of QKD. additionally, as time passes, these devices will only improve and when application specific devices are designed for the MWIR and LWIR, it is reasonable to expect high performance single-photon detectors. These new devises enable investigations into the performance of DV-QKD all across the electromagnetic spectrum.

1.5 Limitations and Motivations

Quantum key distribution has shown tremendous potential to provide provably secure communication and to guarantee privacy for current and future society alike. Optical fibre will be the primary distribution channel for QKD but until commercial quantum repeaters are developed to work around the no cloning theorem, the distance of quantum fibre communication will be limited. In the meantime, quantum satellite communications are seen as a promising alternative to provide long-range QKD and enable a global quantum internet. However, these free-space channels are more complex and less understood than the ground based fibre channels. Signals propagating through the atmosphere are subject to a range of adverse effects that degrade the performance of the system. These phenomena include free-space diffraction, absorption, scattering, turbulence, and background noise, which each serve to limit the secret key generation rate. These effects must be carefully studied to optimise secret key rate and extend the distance of quantum satellite communications. Additionally, to fully democratise the power of quantum technologies, QKD systems need to be able to operate in a variety of atmospheric conditions and geological locations. The key motivations of this research are to compare regions of the electromagnetic spectrum for QKD performance and determine which wavelengths yield the highest secret key rate in a range of atmospheric conditions. To this end, the same detector efficiencies are assumed for all wavelengths as a demonstration of what is possible for each of the wavelengths rather than what devices are currently available on the market. The investigation into longer wave QKD is predicated on three assumptions.

1. The dip in solar radiance at the MWIR could help improve performance in day light conditions and overcome the solar radiation limitation.

2. The superior propagation of the LWIR could overcome the limitations of adverse conditions and generate usable secret key rates when visibility is low.

3. Longer wavelengths in the MWIR and LWIR are less influenced by the negative effects of turbulence than wavelengths in the visible, NIR and SWIR regions.

Chapter 2

Methodologies

2.1 Introduction

Before the background, theory and results of this study are presented, this chapter details some important research design considerations that guide the structure of this thesis and the research it contains. The aim of this chapter is to inform the reader of how this research was designed and how each of the research design choices were decided. It discusses the type of research undertaken, the collection methods, analysis methods and the tools used. The intention is to demonstrate a deep understanding of this topic, improve the replicability of the work and to identify and discuss potential limitations.

2.2 Research Questions

The motivations for this research are to investigate quantum key distribution (QKD) performance in regions of the electromagnetic spectrum that have historically been overlooked due to a lack in cost-effective, fast and efficient devices. Initial research into this topic revealed the dominant narrative in the industry was that the near-infrared (NIR) and short-wave infrared (SWIR) atmospheric windows contained the wavelengths most suitable for satellite quantum key distribution. This is supported by a myriad of research papers utilizing these wavelengths for satellite QKD, as previously discussed in chapter 1. However, the satellite channel faces a number of challenges, namely the reduction in performance due to daylight solar radiation, which has confined experimental investigations to nighttime operation. In addition, the effects of turbulence distort and spread the beam resulting in loss at the receiver while adverse weather conditions absorb and scatter signal photons reducing the secret key rate below usable rates. These limitations motivate research into alternative wavelength regions to see if these challenges can be overcome. The mid-wave infrared (MWIR) experiences significantly less solar and terrestrial radiance than much of the electromagnetic spectrum (0.4 - 12 μm), potentially permitting daytime operation. Meanwhile, longer wavelengths tend to have better propagation through turbulence, resulting in less beam spread and wavefront distortion. Finally the long-wave infrared (LWIR) has been the subject of many research papers claiming superior propagation through adverse weather conditions. Now that single-photon detectors exist across almost the entire spectrum in the form of superconducting nanowire single-photon detectors (SNSPD) and quantum cascade lasers are advanced enough to produce faint laser pulses at infrared wavelength, longer wavelengths can be explored for quantum key distribution.

2.3 Type of Research

Research can be classified by two categories, qualitative and quantitative. In-depth interviews, documentation, focus groups and case study research are all examples of qualitative research approaches. Qualitative approaches produce understandings of how people perceive their social reality and, as a result, how they behave in that world. This work is almost entirely described by quantitative research. Quantitative research entails gathering and analyzing numerical data objectively in order to characterize, predict, or regulate factors of interest. Quantitative research aims to explore causal correlations between variables, make predictions, and to model the physical universe. Through experimentation or numerical simulation, quantitative research attempts to account for extraneous variables to investigate variables of interest while aiming for objectivity. In quantitative research, reality is objective and exists independently of the researcher, who simply plays the role of an observer. The numerical investigations undertaken here are characteristic of quantitative research, an important point to make early on in the research process for informing research design questions as they arise.

2.4 Research Tools

In this section, some of the tools which enabled this research are introduced and discussed. These tools include MODTRAN, MATLAB, and Kay, Ireland's High Performance Computer.

2.4.0.1 MODTRAN

In this work, MODTRAN (MODerate resolution atmospheric TRANsmission) is used to explore different atmospheric transmission windows across the electromagnetic spectrum [73]. MODTRAN is designed to model atmospheric propagation of light for the 200 nm - 100 µm spectral range. Traditionally MODTRAN has used a band model algorithm to approximate radiative transfer using a computational spectral resolution of 0.1 cm^2. MODTRAN has been rigorously validated throughout the course of its 30-year history, and it now serves as the community's standard atmospheric band model. However MODTRAN6 [84] introduces a line by line (LBL) algorithm which allows the transmittance to be computed at an arbitrarily small wavelength resolution by using HITRAN, a high resolution transmission molecular absorption database. This LBL algorithm can be used to validate the much faster band model approximations. It can quantify the amount of absorption and scattering that take place due to gases, aerosols and adverse weather conditions such as fog, haze and precipitation. This allows the Beer-Lambert equation to be resolved for a wide range of conditions. In this work, MODTRAN6 is used to identify channels of high transmission and low spectral radiance. This will help clarify what wavelength ranges are available for QKD by determining the losses resulting from atmospheric extinction (absorption and scattering) while enabling calculations of background noise.

In addition to the base MODTRAN package, the Atmospheric Generation Toolkit enables specific geographical locations to be simulated. It's a separate application that adds additional atmospheres to MODTRAN based on historical and radiosonde data. It allows MODTRAN6 users to quickly and easily enter custom atmospheres into MODTRAN by specifying the latitude and longitude, day of year and time of day. The Atmospheric Generation Toolkit is used in this work to replicate the atmospheres of Waterford and Tucson, allowing location-specific comparisons.

2.4.0.2 High Performance Computing (ICHEC)

The capacity to analyze data and conduct complex calculations at rapid speeds is known as high performance computing (HPC). This research leverages the use of the Irish Centre for High-End Computing's (ICHEC) primary high-performance computer for academic researchers called Kay, which is Ireland's national high-performance computer. Kay enables the use of high-performance computing to develop efficient services and solutions based on technologies such as artificial intelligence, simulated quantum computing, and cyber security to name just a few. In this work, Kay is used to efficiently execute large Monte Carlo loops. Specifically, it is used to generate thousands of individual turbulent paths, enabling ensemble statistic analysis to characterise the propagation path and determine the impact of atmospheric turbulence.

2.4.1 MATLAB

MATLAB is a computer language that engineers and scientists use to study and build systems or numerical models. MATLAB provides a matrix-based language that allows computational mathematics to be expressed in an intuitive way. The matrix-based nature of the language makes it ideal for working with large arrays, as is the case in this thesis.

2.5 Data Collection

The following section is a discussion regarding the techniques used throughout this research for the purposes of data collection. Data gathered in this work is primarily generated through the use of simulation packages such as MODTRAN and numerical models such as the phase screen model or BB84 QKD protocol, developed and implemented in MATLAB. A brief summary of each is given.

To accurately account for the wavefront distortions induced by atmospheric turbulence, some numerical simulations of the propagating beam are required. To this end, the phase screen model is adopted [85][86]. In the phase screen model the propagation path is subdivided into smaller regions and the random phase changes of each region are accounted for by a thin phase screen placed at the beginning of each region [87]. In this model, the free space beam spread is separated from the phase perturbations and applied to the beam separately, allowing each effect to be simulated using the most computational efficient technique. Turbulence is a statistical model and should be simulated using some statistically distribution to reflect that. For that reason, the phase screen model is implemented on Kay (Ireland's HPC) where each statistically independent path is simulated separately and ensemble statistics are then used to characterise the turbulent path. More information is given on the phase screen model in chapter 3 but for now it is enough to know that through numerical modelling, the phase screen model allows the wavefront distortion and turbulence-induced beam spread to be quantified [50]. The reason for using the phase screen model over alternative numerical turbulence models is the computational efficiency of the Fast Fourier Transform (FFT). The phase screen model allows the turbulent path to be reconstructed and the effects on the beam are numerically replicated through statistical realisations of the turbulent path, allowing detailed investigations into the nature of the wavefront distortions. This allows detailed characterisation of the turbulent effects but ultimately this model is too computationally intense to be used in the channel model. Instead, it is used to describe the distortion of the beam at different wavelengths which is summarised using the Strehl ratio, a metric describing the quality of the wavefront. This means that the phase screen model does not need to be run every time the channel is simulated but instead is used as a validation tool.

The Atmospheric Generation Toolkit is used to generate location-based atmospheric data which can be fed into MODTRAN to determine the atmospheric absorption, scattering and spectral radiance for a range of wavelengths. To establish the global quantum internet, the satellite QKD channel must achieve high secret key rates in a variety of atmospheric conditions and geographical locations. For that reason, two very different atmospheric and geographical scenarios are considered. Waterford, Ireland (52.2593° N, 7.1101° W) is used to represent geographical locations which are not typically suitable for satellite communications due to the poor weather and high cloud coverage. Before thick clouds are investigated, a relatively clear Winters day is considered, using a cirrus cloud model. The Winter solstice was chosen as the day of the year and 12 pm noon was selected as the time of day. Although Waterford is a small city, the receiver location will be stationed in the country side so a rural aerosol model is implemented in MODTRAN, using the default 23 km visibility. Additionally, farm albedos are used to replicate rural Waterford vegetation. In contrast, 70 km visibility represents clear skies at 12 pm noon on the summer solstice in Tucson, which is selected as a more ideal location for satellite communications. The summer solstice is selected to determine if QKD performance is possible when solar radiation is at a maximum. A desert aerosol model is combined with desert albedos and 3.33 m/s wind speeds to replicate the dry, humid Tucson environment. These locations were chosen in an attempt to demonstrate differential performance across each wavelength region and to determine if there is a significant difference in QKD performance for varying wavelengths in different locations and conditions.

When a MODTRAN simulation is complete, the data is stored in a .json file. This file is imported into MATLAB to extract the transmittance and radiance across the investigated region. Once in MATLAB, the wavelengths are deconstructed into channels, who's width depends on the size of the spectral filter used. The radiance and transmittance for each channel is an average of the values within that spectral filter width and the wavelength is now the centre wavelengths of that channel. Inside the MATLAB script, the signal to noise ratio and secret key rate are calculated for each channel using the BB84 decoy-state protocol. The BB84 protocol is one of the most widely used protocols and used here as a general validation of quantum communication performance. The decoy-state method is used to replicate the typical physical implementations which require protection against photon number splitting attacks. The channel model is complimented with the Turbulence Limited (TL) filtering strategy described in [52], which imposes a spatial filter to block noise photons and permit daytime operation. The reason for focusing on the downlink rather than the uplink is in line with current state of the art experimental realisations which unanimously use the downlink due to a huge reduction in turbulence loss. However, the uplink remains a point of consideration due to the advantages of longer wave propagation through turbulence and should be the subject of further research. For each channel, the model combines the losses resulting from diffraction, atmospheric extinction and turbulence to determine the channel efficiency. Similarly, the spectral radiance and spatial filter field of view are used to determine the background probability for each channel. The performance of each wavelength channel is highly correlated to the choice of initial beam waist and receiver size so these two parameters are also varied to find the best wavelength-receiver-initial beam waist combination.

2.6 Data Analysis

Previous work analysing QKD performance while varying the wavelength resulted in plots with wavelength on the x-axis and secret key rate on the y-axis, providing a simple graphical comparison. While this can be useful to identify the best wavelength for a particular set of parameters, it is clear that secret key rate optimization is a multivariate problem and the best wavelength only exists for a given set of parameters. A fair wavelength comparison cannot be done in isolation but instead requires a number of other parameters to be varied concurrently. While there are many parameters that can be varied alongside wavelength, it is the focus of this work to vary the transmitter and receiver component sizes. Specifically, the physical limitations are investigated in the form of variable initial beam waists and receiver aperture diameters, which ultimately determine the geometric coupling loss and the amount of background noise that enters the detector. If the main aim of this work was to find the highest achievable secret key rate then the initial beam waist, receiver size and wavelength should be optimised together. However, the goal is to compare the performance of each transmission window and present the results in a way that is easily digestible for the reader. This requires a four-dimensional graphical representation which does not work well considering the size of each array, where thousands of channels are compared on the same plot. A three-dimensional surface plot serves as a much more elegant representation of the results. However, only two variables can be compared at a time so first the initial beam waist is made constant, while the receiver size and wavelength are varied. This choice was made because the initial beam waist only affects the diffraction of the beam, scaling the geometric loss at the receiver. In contrast, the receiver diameter also scales the geometric loss while directly controlling the amount of background noise, leading to a trade-off design consideration. Wavelength affects almost every aspect of the channel, imposing its own set of design considerations. Two initial beam waists are chosen, 10 cm to replicate the size limitations imposed by a CubeSat and 35 cm to show what is possible if a larger satellite is utilized. For these two conditions, the receiver size and channel centre wavelength are varied together to find what wavelengths produce the highest secret key rates. Once these wavelengths are identified, then the initial beam waist and receiver size are optimised together to find what combination produces the highest secret key rate. This enables optimisation of two variables at a time and the three-dimensional results can be plotted while also identifying the highest performing initial beam waist, wavelength and receiver for each transmission window.

The 3D surface plots allow the huge arrays of results to be displayed in an easily understood format. Rather than providing the results for a set of components, it demonstrates the performance of the system across a range of components, informing the reader of all possible scenarios, offering insights into important design considerations for the satellite link. With the best case for each window identified, the regions are compared to find which achieves the best performance across a wide range of conditions including the clear sky of Tucson, some light clouds in Waterford, a range of turbulence strengths as well as a number of adverse weather conditions including fog and haze. This provides clarification on which wavelengths are best suited for satellite quantum key distribution when the optimum components can be utilized. However, in real applications there are often component size limitations imposed by the satellite payload, ground station and the cost of devices. To account for this, the best wavelengths within the 0.4 - 12 μm region are identified at each receiver size so that researchers can identify the best wavelengths for their particular component size limitation.

2.7 Scope of Research and Summary of Methodology

The contributions of this work are to determine which regions of the electromagnetic spectrum produce the highest secret key rates for satellite QKD downlink channels operating in daylight under realistic and adverse geometric and atmospheric conditions. To achieve this goal we investigate a variety of atmospheric scenarios across a wide range of wavelengths. First, a channel model is developed accounting for free-space diffraction, turbulence and background noise to enable calculations of secret key rate using the decoy-state BB84 protocol [17]. The wavelengths are separated into regions and further divided into channels characterised by the channel's centre wavelength λ, and channel width $\Delta\lambda$, determined by the size of the receiver spectral filter. Next, the simulation results are analysed to identify what wavelength regions are suitable for satellite QKD. The transmitter and receiver apertures are optimized with wavelength to account for the effect that the initial beam waist w_0, and the diameter of the receiver aperture D_r, have on wavelength selection and secret key rate optimization. Using this framework the best λ, D_r, w_0 combinations are selected from each region and used to represent their respective atmospheric windows in comparison through varying turbulent strength. This serves to give an example of what is possible in terms of maximising QKD performance. However, for practical QKD there is often limits imposed on receiver and transmitter sizes so the best wavelengths for a range of component sizes are determined. This provides an overview of what wavelengths achieve the best performance as the transmitter and receiver sizes are varied allowing researchers to optimize the performance of their specific system. Finally, the performance of each wavelength region is compared while operating through adverse weather conditions such as haze, fog and rain.

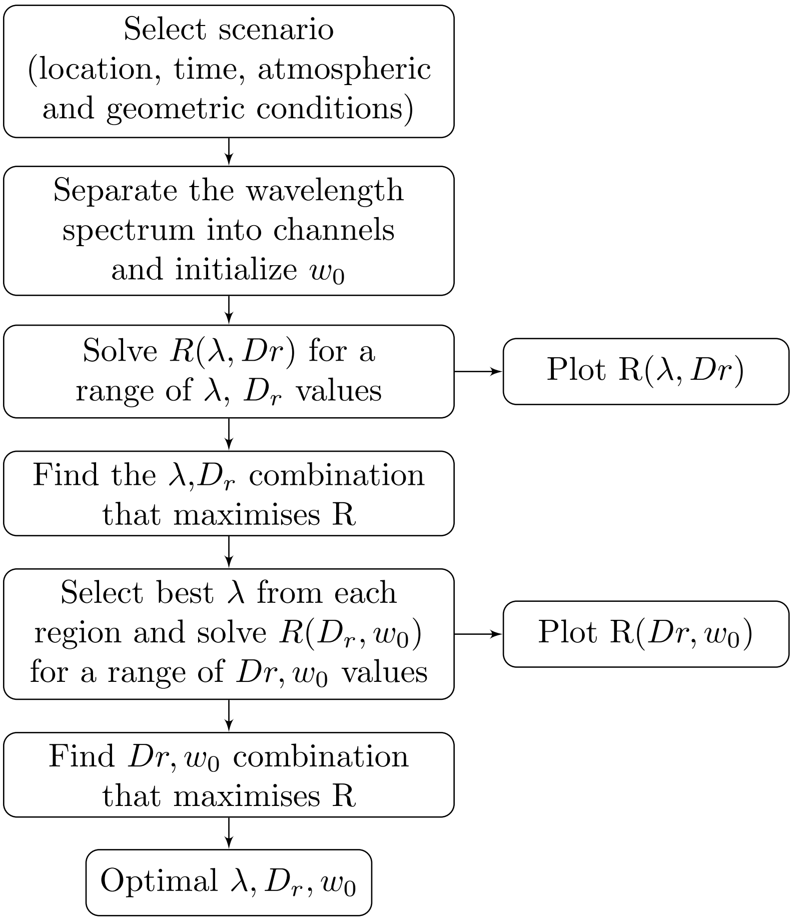

Select scenario (location, time, atmospheric and geometric conditions)
Separate the wavelength spectrum into channels and initialize w_0
Solve $R(\lambda, Dr)$ for a range of λ, D_r values
Plot R(λ, Dr)
Find the λ,D_r combination that maximises R
Select best λ from each region and solve $R(D_r, w_0)$ for a range of Dr, w_0 values
Plot R(Dr, w_0)
Find Dr, w_0 combination that maximises R
Optimal λ, D_r, w_0

Figure 2.1: Methodology used to find the best wavelength λ, receiver diameter D_r, and initial beam waist w_0, for each transmission window while providing a visual representation of how these variables effect the secret key rate R.

Our analysis seeks to compare the suitability of each channel for satellite QKD by calculating the secret key rate R, as a function of λ, D_r and w_0. Rather than simply determining which combination of values achieves the highest performance, we wish to support the system design process by providing a visual comparison of all channels for a range of D_r and w_0. As there is no effective way to display 4-dimensional arrays we instead set one variable to a constant value and then determine R as a function of the two remaining variables. The methodology described in Fig. 2.1 exploits the fact that w_0 has more effect on the required receiver aperture and maximum key rate than it does on wavelength selection. This allows us to set w_0 to a constant value and solve R for a range of λ and D_r values. The resulting 3D array can be presented graphically using surface plots with λ and D_r on the x and y axes and the corresponding R shown using a colour gradient. Allowing D_r to vary prevents it from limiting channel performance and enables a fair wavelength comparison. For each wavelength region the highest performing λ is selected and used to solve R for a range of D_r and w_0 values. The resulting 3D array is plotted and the optimal D_r, w_0 is found for the chosen wavelengths providing a best-case scenario comparison. A number of design considerations were discussed in this chapter, describing the motivations and reasoning behind the most important decisions that dictate the direction of the research. The information delivered is important for insuring the integrity of the research while documenting the methodologies used allows the work to be replicated and validated. The following section provides a theoretical description of the channel model and presents the relevant background information necessary to understand this research.

Chapter 3

Theory

This chapter provides an understanding of the relevant theory used throughout the rest of the thesis. First, the satellite-earth channel is discussed in the context of classical communications to reveal the phenomena that affect the beam as it propagates. Next, the discussion is extended to include quantum communication, where some rudimentary quantum mechanics is introduced to help explain the BB84 decoy-state protocol. The chapter concludes by developing a channel model which will be used to determine the secret key rate in chapter 4.

3.1 Classical Communication

This research is focused on exploring the relationship between wavelength and the performance of satellite-based quantum key distribution. While this will ultimately be determined using a secret key rate calculation, it is helpful to separate the discussion into classical and quantum communication. In this section, the detrimental phenomena affecting classical satellite communications are discussed and used to build a model of the channel.

3.1.1 Atmospheric Extinction

One of the biggest loss factors in the satellite channel is atmospheric extinction. Atmospheric extinction can be described as the attenuation experienced by a beam as it propagates through the atmosphere. The troposphere ($\approx$ 0 - 10 km), stratosphere ($\approx$ 10 - 50 km), and mesosphere ($\approx$ 50 - 86 km) are the lowest three atmospheric levels in terms of geometric altitude [88]. Satellite to ground links also include propagation through the ionosphere (50 - 1,000 km), however, ionospheric effects are insignificant beyond 2 GHz so they are not taken into account in this work [69]. Most atmospheric effects are only relevant below the Karman line, approximately 100 km above earth's surface. The attenuation arising from atmospheric extinction is driven by two effects, atmospheric absorption and atmospheric scattering, which together describe the Beer–Lambert law, given by the following equation [89]

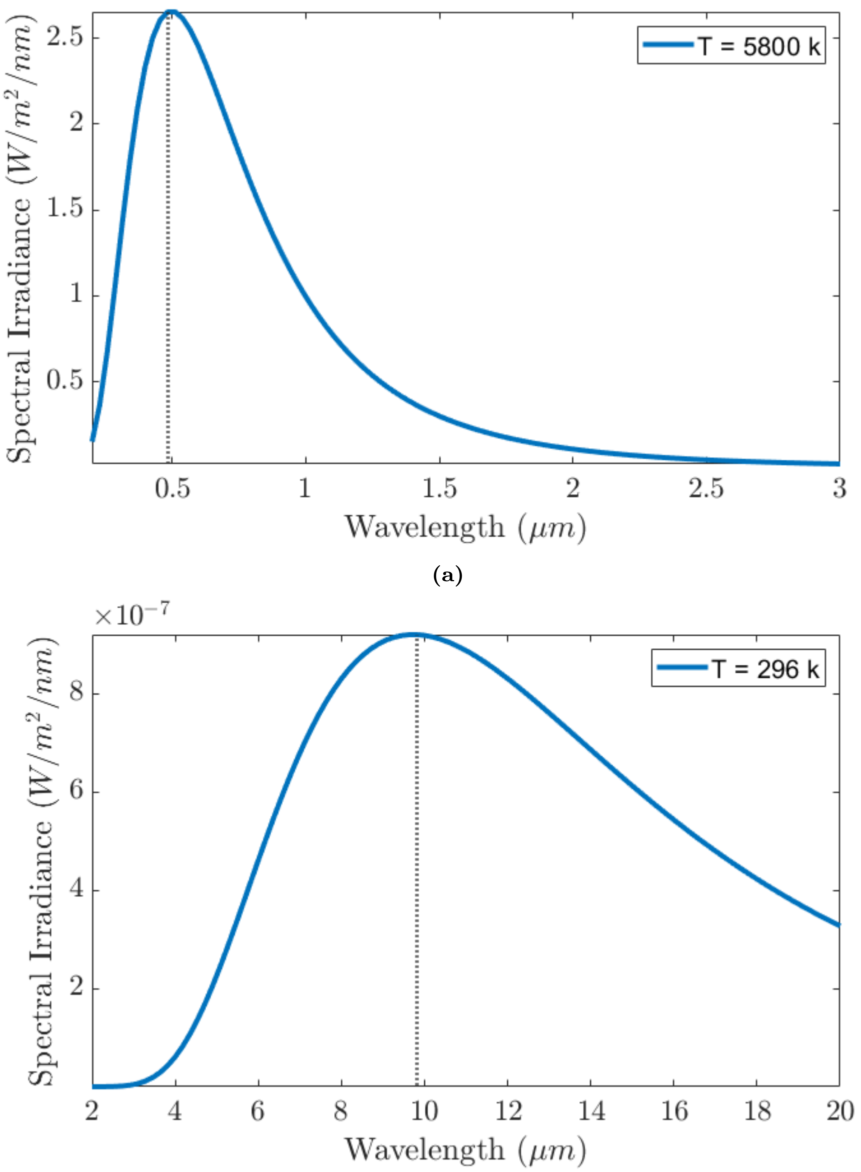
$$\tau_a = \exp^{-(\beta_{abs}+\beta_{scat})R} \tag{3.1}$$

where β_{abs} and β_{scat} are the absorption and scattering coefficients and R is the optical depth of the atmosphere. Molecular absorption is a process that can occur when light interacts with a molecule, resulting in that molecule absorbing light energy of a certain wavelength, allowing the molecule to move from the ground state to higher energy excited states [90]. Different molecules in the atmosphere absorb light of different wavelengths, making molecular absorption a critical consideration in wavelength selection. Nitrogen and Oxygen are the most abundant gases in the atmosphere but neither have absorption bands in the infrared spectrum [88]. In contrast, Oxygen along with Ozone and water vapour are the primary absorbers in the visible spectrum. Indeed, water vapour is big contributor to overall absorption across many regions of the electromagnetic spectrum. Interestingly, water vapour concentration is highly variable depending on geographical location, time of day and time of year, which means that atmospheric absorption is also variable and dependent on these same variables. The high freezing point of water yields a significant dependence on temperature which indirectly makes water vapour concentration variable with respect to altitude, resulting in most of the water vapour absorption occurring at lower, warmer altitudes and locations. Atmospheric absorption and scattering are both highly wavelength-specific so access to a molecular spectroscopic database like HITRAN [70] is necessary for determining the absorption and scattering coefficients, β_{abs}, β_{scat}, as described by Lambert-beer's law. Indeed a number of simulation tools have been developed to access such databases and extract absorption and scattering coefficients. Examples of such software packages are the LBLRTM algorithm mentioned in chapter 1 and the prominent Air Force Geophysics Laboratory (AFGL) codes FASCODE, MODTRAN, and LOWTRAN, which are quantum-mechanical models that describe molecular absorption and scattering. MODTRAN6 is used throughout the course of this thesis to calculate atmospheric extinction via molecular absorption and scattering.

The two types of scattering that are most relevant to atmospheric propagation are molecular scattering due to interactions between light and the molecules that constitute the air, and scattering by solid particles or liquid droplets suspended in the air. Rayleigh scattering is the name given to molecular scattering because it was first researched and explained by Lord Rayleigh. The primary cause of scattering via suspended particles is due to aerosols in the atmosphere, hence this type of scattering is often called Aerosol scattering or Mie scattering named after Gustav Mie. Adverse weather such as fog and haze are also major contributors to Mie scattering. Rayleigh scattering dominates when the size of the molecule is much smaller than the incident wavelength while Mie scattering usually occurs when the particle diameter is of comparable size to that of the incident wavelength. Non-selective scattering is less common in this channel and applies when the particles are much larger than the incident wavelength. Rayleigh scattering tends to affect the visible and some of the NIR more than it does for SWIR, MWIR and LWIR wavelengths. However, Mie scattering is more prominent in the infrared wavelength range. Additionally, Mie scatter tends to occur in the lower atmosphere, where bigger particles are more prevalent, and it predominates when the sky is overcast.

3.1.2 Spectral Radiance

Another wavelength-dependent loss factor is the background noise received by the detector. While detector dark counts play a role, the background noise is dominated by spectral radiance



(a)

(b)

Figure 3.1: Black body spectrum using Wiens Displacement Law to estimate the spectral radiation emitted by (a) the sun and (b) the earth, using temperatures of 5800 K and 296 k respectively.

originating from external sources such as the sun, moon and earth. Radiation emitted from block bodies exists as some wavelength distribution depending on the temperature of that body. If we treat the sun and earth as black body radiators of temperatures 5800 k and 300 k respectively, then the sun will have a peak in radiation at approximately 483 nm while the earth will peak at approximately 9.8 μm. The spectrum is determined using Wiens Displacement Law and used to plot the black body equivalent solar and terrestrial radiation in Figure 3.1. While neither the sun nor the earth are perfect black body radiators, these curves serve as a good indication of the spectral radiance across the spectrum. While solar radiation is mainly emitted in the visible and NIR wavelengths, terrestrial radiation is primarily emitted in the infrared. While these plots are useful for visualizing the radiation across the spectrum, more accurate results can be generated using MODTRAN. MODTRAN simulates spectral radiance emerging from multiple sources and combines them to estimate the total spectral radiance at the receiver. The amount of radiation that reaches the receiver follows some statistical distribution such that the total radiance varies for each MODTRAN simulation. Thus the software must be run a number of times in order to uncover the probability distribution which informs calculations of total background probability, shown later in this work. Additionally, radiance varies substantially as the suns relative position to the earth changes, such that the time of day, day of the year and geographical location are significant MODTRAN input variables for calculating total radiance. Before any calculations of secret key rate can be discussed, a specific time, day and location must be decided so that the relevant spectral radiance can be obtained.

3.1.3 Free-space diffraction

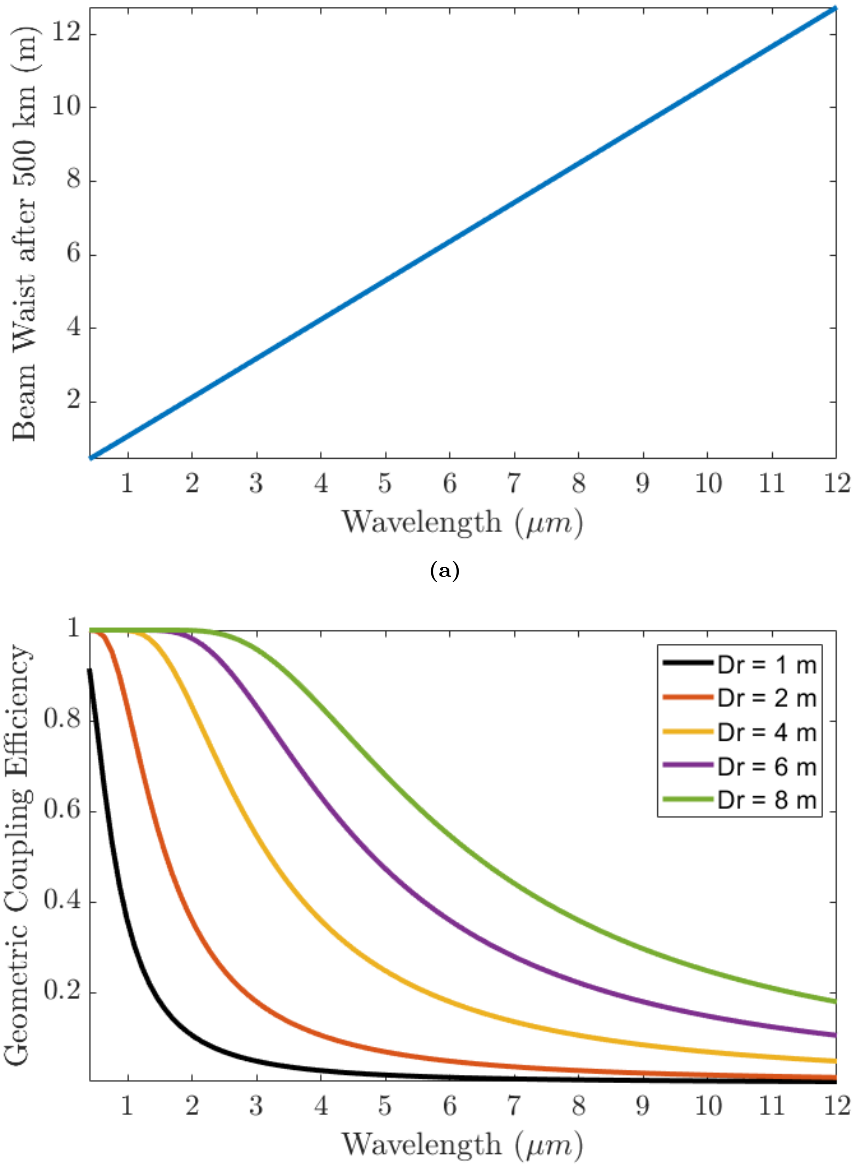
The biggest source of loss in the free space satellite downlink channel is due to diffraction-induced beam spread. LEO satellites are expected to form the backbone of satellite-based quantum communications, with 500 km being a suitable altitude. Signals will have to travel hundreds of kilometres before they reach the receiver and as the beam propagates its intensity distribution will begin to spread. By the time the beam reaches the receiver, the beam waist will be very large and much of the signal can be lost. It is common practice to approximate a laser beam as a Gaussian beam where the transverse intensity profile follows an ideal Gaussian distribution. As the beam propagates, diffraction causes its profile to change depending on its wavelength, initial beam waist and propagation distance. The beam spot size radius for a Gaussian beam with wavelength λ, at a distance z, is given by [91]:

$$w(\lambda, z) = \sqrt{w_0^2 \left[1 + \left(\frac{\lambda z}{\pi w_0^2}\right)^2\right]} \tag{3.2}$$

where w_0 is the initial beam waist. It is this increase in the beams spot size relative to the size of the receiver aperture that is responsible for significant power loss in the satellite downlink scenario. This free-space diffraction-induced loss can be accounted for using the following equation [92]

$$\eta_d = 1 - \exp\left(-\frac{1}{2}\frac{D_r^2}{w^2(\lambda, z)}\right) \tag{3.3}$$

where D_r is the diameter of the receiver aperture. This equation assumes perfect alignment between the satellite transmitter and the terrestrial receiver. While it is important to include losses associated with an Acquisition, Tracking, and Pointing (APT) system, it is beyond the scope of this work but may be added to the model in the future. The relationship between beam waist radius and wavelength is calculated using equation 3.2 and shown in Figure 3.2 (a). The beam waist size at the receiver determines the geometric coupling efficiency via equation 3.3, which is shown graphically in Figure 3.2 (b). In both cases, a 15 cm initial beam waist is used to determine the beam waist and geometric coupling efficiency into a number of different receiver aperture sizes, after 500 km propagation using wavelengths across the electromagnetic spectrum. The size of the beam waist at the receiver increases linearly with wavelength but the geometric

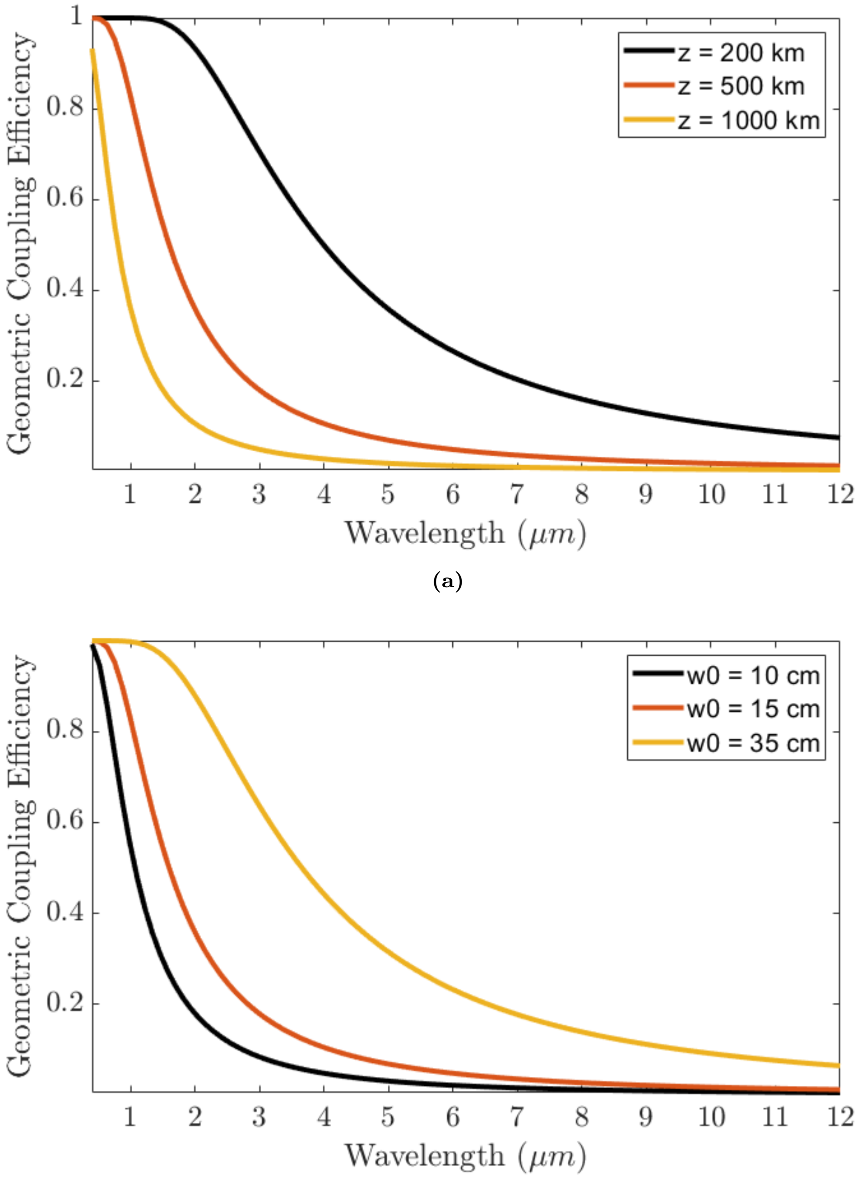


(a)

(b)

Figure 3.2: Plot showing the relationship between wavelength and (a) beam waist and (b) geometric coupling efficiency for a 15 cm initial beam waist and 500 km propagation distance.

coupling efficiency declines exponentially as wavelength is increased and as the receiver size is decreased. This demonstrates the need for larger components when using the MWIR and LWIR regions. Note that the LWIR has a geometric coupling efficiency of less than 10 % if a 2 m aperture is used, in contrast to almost 100 % geometric coupling efficiency in the visible and NIR with the same 2 m aperture diameter. Provided that atmospheric transmission windows are used and the atmospheric extinction losses are low, the geometric coupling efficiency will drive the channel efficiency and ultimately the secret key rate. Optimising equation 3.3 to minimise diffraction-induced beam spread loss, is one of the best ways to maximise secret key



(a)

(b)

Figure 3.3: Highlighting the relationship between a) the propagation distance and b) the initial beam waist, with the geometric coupling efficiency.

rate generation. In Figure 3.3 (a), three propagation distances are considered as the wavelength is varied across the spectrum, to demonstrate satellite altitude as a design consideration. As expected, increasing the propagation distance allows the beam waist to spread even more and reduces the geometric coupling efficiency. Similarly in Figure 3.3 (b), three initial beam waists are used to calculate the geometric coupling efficiencies across the same range of wavelengths, to reveal the huge impact that initial beam waist choice has on the channel efficiency. Once again the efficiency in the MWIR and LWIR is poor if the smaller 10 cm and 15 cm initial beam waists are used but increasing the initial beam waist to 35 cm yields a massive improvement across the spectrum.

3.1.4 Turbulence

As the beam propagates through the atmosphere it may encounter atmospheric turbulence caused by random fluctuations in temperature and pressure. This alters the spatial and temporal refractive index of air which in turn can cause the beam to spread and become distorted. The scintillation index (σ_I^2) is a useful measure to quantify the strength of atmospheric turbulence, it is defined as the normalized variance of irradiance fluctuations [50]

$$\sigma_I^2 = \frac{\left\langle I\left(x_0, y_0\right)^2\right\rangle}{\left\langle I\left(x_0, y_0\right)\right\rangle^2} - 1 \tag{3.4}$$

where $I\left(x_0, y_0\right)$ is the received irradiance at the point x_0, y_0. The effects of turbulence on a propagating beam will differ significantly between uplink and downlink due to interactions between the beam spot size and the size of the turbulent eddies. Most turbulent effects occur within the lower 20 km of atmosphere, so the uplink beam encounters turbulence when its waist is still small and susceptible to beam wander and beam spread. In the downlink, the beam travels hundreds of kilometers before it interacts with significant turbulence, at which point the beam waist is large and more resilient against both beam wander and beam spread.

The widely accepted theory of turbulence originally proposed by Kolmogorov, has consistently shown agreement with observation [93] and is used here to analyse the impact that turbulence has on a propagating beam. As the earth rotates around the sun, differential heating and cooling cause variations in the temperature of air which in turn generates wind. Air of different temperatures mixes and forms randomly distributed pockets of air with variable temperatures and size called turbulent eddies. As the density of air depends on its temperature, and its refractive index is dependant on its density, the atmosphere will have a random refractive index profile [86]. Kolmogorov described turbulent flow as a transfer of kinetic energy from large eddies to small eddies. These eddies are characterised by an outer scale L_0, the average size of the largest eddies and an inner scale l_0, the average size of the smallest eddies. Turbulence is a statistical process and so to account for the random fluctuations in refractive index, a spectral density function is used. While there are a number of suitable models for the refractive power spectral density, here the modified von Karman Power Spectral Density (PSD) function is implemented as it is the simplest model that includes both the inner and outer scales [86] [94].

$$\Phi_\phi(k) = 0.49{r_0}^{-5/3}\frac{\exp(-k^2/k_m^2)}{(k^2+k_0^2)^{11/6}} \tag{3.5}$$

where $k_m = 5.92/l_0$, $K_0 = 2\pi/L_0$ and r_0 is the fried parameter for each region given by

$$r_0 = (0.423k^2 sec(\zeta)\int_{h-}^{h+} C_n^2(h)\,dh)^{-3/5} \tag{3.6}$$

where k is the wavenumber and $C_n^2(h)$ describes the refractive index structure of the atmosphere. The Hufnagel-Valley $HV_{5/7}$ model is often used to represent the refractive index structure of the atmosphere and is determined using the following equation [95]

$$C_n^2(h) = 0.00594(\frac{v}{27})^2(10^{-5}h)^{10}\exp\left(-\frac{h}{1000}\right) + 2.7x10^{-16}\exp\left(-\frac{h}{1500}\right) + A\exp\left(-\frac{h}{100}\right) \tag{3.7}$$

for a given wind speed v. It can be shown that for zenith angles less than 60 degrees, the channel operates within the weak turbulence regime ($\sigma_I^2 < 1$). The empirical Coulman-Vernin profile [96] is used to compliment this model, incorporating an altitude dependence for the size of the largest eddies,

$$L_0(h) = \frac{4}{1 + (\frac{h-8500}{2500})} \tag{3.8}$$

and allowing calculations of the outer and inner scales, where $l_0 = 0.005L_0$. To simulate the effect that atmospheric turbulence will have on a propagating beam, the phase screen model [85][87][86][50] is deployed, where the propagation path is subdivided into smaller regions and the random phase changes of each region are accounted for by a thin phase screen placed at the beginning of each region. This model is a physical interpretation of the well known split-step method which is used here to rewrite the parabolic equation as a linear sum of several equations each representing separate propagation effects [97]. This allows the phase perturbations to be isolated and represented using phase screens while using the angular spectrum form of the Fresnel diffraction integral to propagate the wavefront between subsequent screens via 2-D fast Fourier transform. The beam is represented by a two-dimensional square grid of complex numbers corresponding to the value of the electromagnetic field at that point in space [50]. The accuracy of this model depends on the method of phase screen generation. While a number of methods have been used in the literature [98], here the 2-D Fourier Transform technique is augmented with the subharmonic method to improve low spatial frequency representation. The phase screens are produced by performing FFT over a 2-D uniform grid of Gaussian white noise with variance given by equation 3.5 [86]. To ensure that the condition of weak turbulence is maintained across each phase screen, the Rytov parameter is kept constant for each region of turbulence using the following equation [99]

$$r_R^2 = 1.23k^{7/6}\int_{h^-}^{h^+} C_n^2(h)\left(h - h^-\right)^{11/6} dh = b \tag{3.9}$$

where b is set to 0.2 in accordance with reference [50]. The effect of turbulence can be considered negligible above 20 km so equation 3.9 results in the total atmospheric turbulence spread across 17 phase screens. Figure 3.4 shows a graphical representation of three such phase screens which account for the turbulent effects experienced by a subsection of the overall propagation path. The value of each pixel is random and follows the statistical distribution described by equation 3.5.

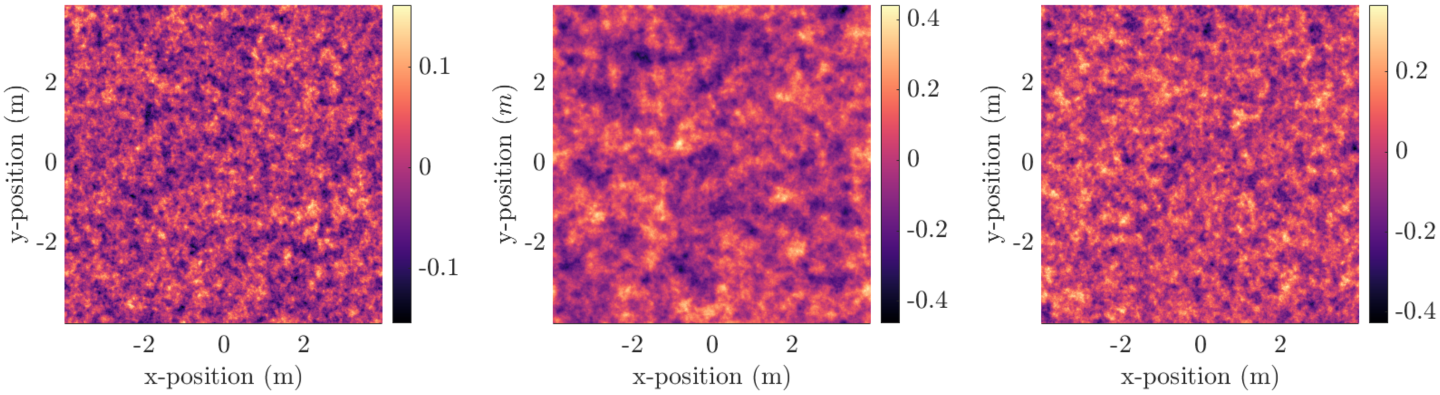


Figure 3.4: Graphical representation of three phase screens which account for the turbulent effects experienced by a subsection of the overall propagation path.

Now that the input parameters have been set up and the properties of the bulk atmosphere have been projected onto the phase screens, the turbulent path can be simulated. As the phase screens are statistically independent, each time the beam is propagated from source to receiver, it travels through a different turbulent path. So to get a meaningful output, the simulation is set up to run in a 10,000 iteration Monte Carlo loop and the outputs correspond to ensemble-averaged statistics. This allows the turbulent channel to be characterised by calculating irradiance fluctuations and average transmissivity. The beam is initialized using a Gaussian function and represented by a uniform 2-D square grid where the value of each pixel corresponds to a complex number describing the electromagnetic field at that point in space [50]. As this is a downlink scenario, the beam is first propagated from the satellite at an altitude of 500 km, to 20 km above the earth's surface where the turbulent effects start to impact the beam. The space between the satellite and the 20 km altitude is treated as a vacuum as is the space between each phase screen. The beam is propagated using a Discrete Fourier Transform (DFT) algorithm to solve the angular spectrum form of the Fresnel diffraction integral and the phase screens apply the phase changes subsequently along the turbulent propagation path. A cross-section of the intensity profile of the beam is extracted at three points throughout the propagation path and shown in Figures 3.5 and 3.6. The x and y axis represent the physical space encompassed by the beam while the colour bar indicates the intensity of the electromagnetic field at each point in space. Figure 3.5 shows the evolution of a 1.55 μm beam as it propagates from the 500 km altitude satellite down through the lower 20 km of turbulent atmosphere. The intensity distribution is similar in the case of the initial beam and the beam after the 480 km vacuum propagation with the main difference being the size of the beam, which has grown tenfold. The remaining 20 km of turbulent propagation have little effect on the size of the beam but significantly affects its phase which results in a distorted wavefront where the strength of the electromagnetic field is concentrated in pockets of high intensity. Similarly, Figure 3.6 shows the evolution of a 10 μm beam as it propagates from a 500 km satellite to a ground-based

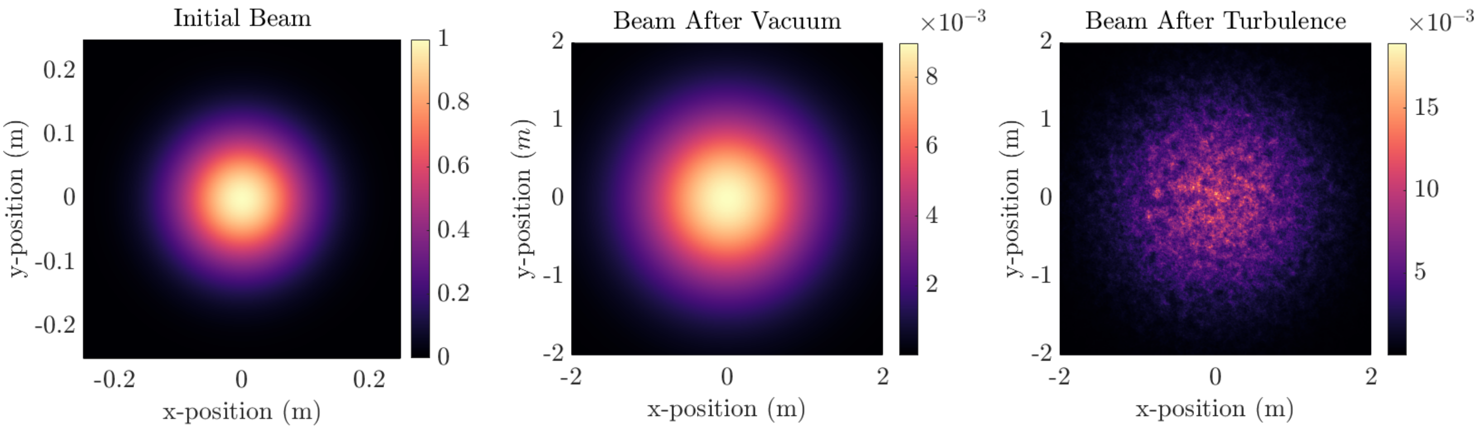


Figure 3.5: The intensity profile for a 1.55 μm beam at initialization (left), after a 480 km vacuum propagation (middle) and after a 20 km turbulent propagation path following the 480 km vacuum propagation (right).

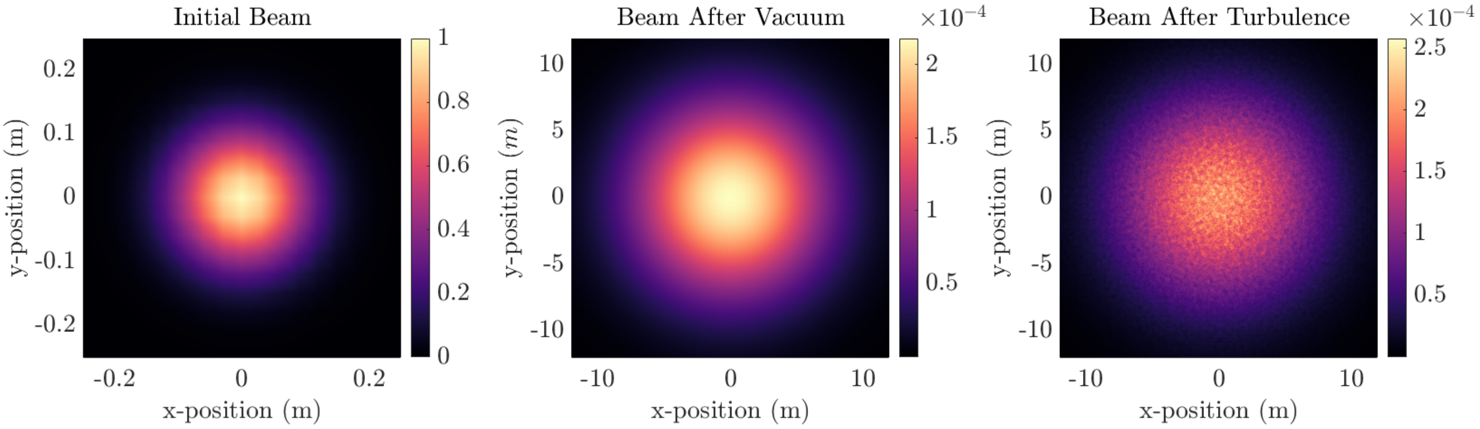


Figure 3.6: The intensity profile for a 10 μm beam at initialization (left), after a 480 km vacuum propagation (middle) and after a 20 km turbulent propagation path following the 480 km vacuum propagation (right).

receiver. Note that no attenuation from atmospheric absorption or scattering is considered in these figures, they serve to isolate the impact of turbulence to quantify its effect on the beam. Once again, the beam waist remains largely unchanged but notice a significant improvement in the wavefront of the 10 μm beam in contrast to the 1.55 μm. The LWIR wavelength is far less effected by turbulence than the SWIR wavelength, highlighting the benefit of using longer wavelengths in turbulent conditions. Although the LWIR wavefront is distorted, the beam maintains much of its original Gaussian structure.

While it is clear from Figures 3.5 and 3.6 that the turbulence-induced beam spread is very low in the downlink scenario, it is not enough to say the spread is negligible. To quantify the amount of beam spread, the beam waist of the intensity distribution at the receiver plane must be measured. Although the wavefront is distorted, it still possesses a circular Gaussian intensity profile where the beam waist can be defined as the circular area that encompasses all but $1/e^2$ of the total power. To measure the beam waist, a small circular aperture is applied at the receiver plane and the receiver power is measured. The circular aperture is incrementally increased until $1 - 1/e^2$ of the power is received. Thus the beam waist is the circular aperture that allows 86.47 % of the total power at the receiver plane to pass through the aperture. In Figure 3.7, the impact of turbulence is compared by contrasting two models, the first is the beam spread resulting from diffraction-induced free space spread in a vacuum as determined by equation 3.2 and the second is the beam spread resulting after 480 km of vacuum propagation plus 20 km of turbulent propagation, determined using the phase screen model. The phase screen algorithm is run 10,000 times on a high performance computer for a number of different wavelengths to determine the average beam waist resulting from this satellite downlink propagation, when the initial beam waist is 15 cm, the zenith angle is 0 and the effects of atmospheric turbulence are considered negligible above 20 km. The average beam waist for a number of wavelengths is represented by red circles in Figure 3.7 in contrast to the blue line representing the beam spread induced by diffraction in a vacuum calculated using equation 3.2. Additionally, the power loss resulting from beam spread is compared in Figure 3.8 for both vacuum and turbulent propagation. The loss is a result of the receiver being too small to capture all the power in the beam, in the case of vacuum propagation it is calculated using equation 3.3 (solid lines) while the loss for the turbulent propagation is determined using the phase screen model (circles). Two receiver apertures are considered, 2 m (black) and 4 m (red) and the ratio between power sent and power received is converted to dB. As expected, the larger aperture experiences less loss as do the smaller wavelengths. This plot serves as further verification that turbulence-induced beam spread can

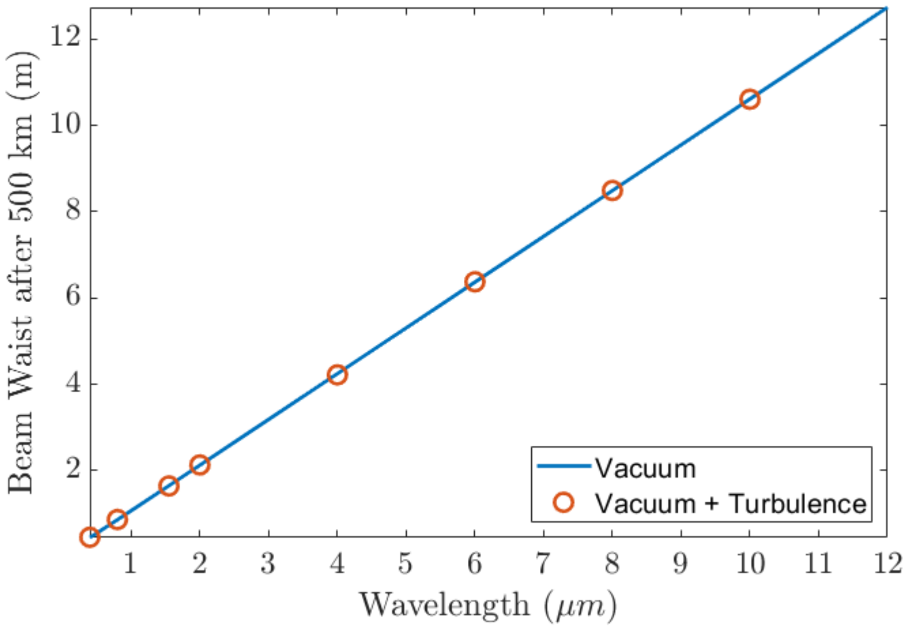


Figure 3.7: Beam waist after 500 km vacuum propagation compared to the beam waist after 480 km of vacuum propagation plus 20 km of turbulent propagation.

be considered negligible in the downlink scenario. These results are in agreement with recent

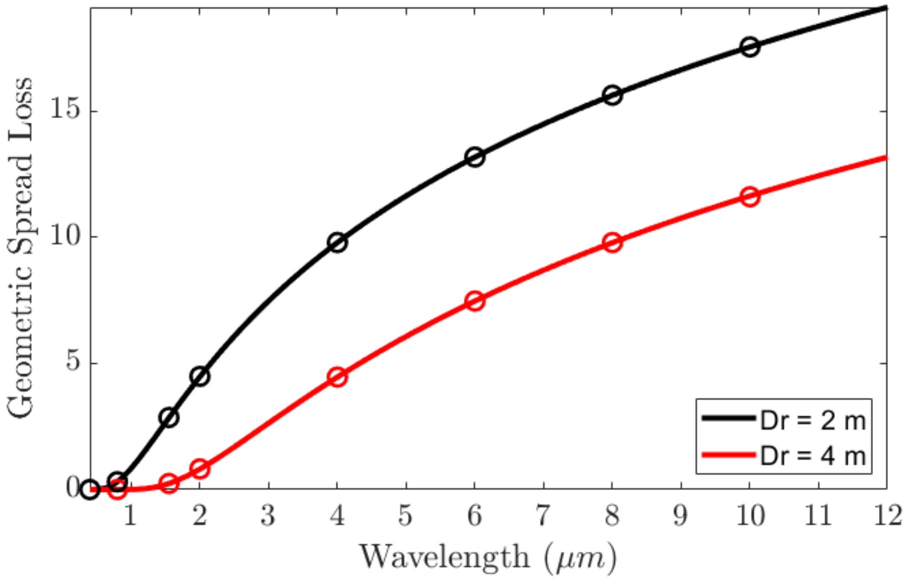


Figure 3.8: Beam spread loss after 500 km vacuum propagation (solid lines) compared to the beam spread loss after 480 km of vacuum propagation plus 20 km of turbulent propagation (circles) using two aperture sizes, 2 m (black) and 4 m (red).

findings from a 2021 paper by Stefano Pirandola [40] which showed that once the system is operating under conditions of weak turbulence and low zenith angles, the effects of atmospheric turbulence on beam spread can be considered negligible. The final spot size or long-term spot of the beam is a combination of diffraction-induced spread and turbulence-induced spread and can be written as

$$w_{\mathrm{lt}}^2 \simeq w_d^2 + 2\left(\frac{\lambda z}{\pi \rho_0}\right)^2 \tag{3.10}$$

where w_d is determined using equation 3.2 and the spherical-wave coherence length coherence for a propagation of length z, is defined at zenith as [40]

$$\begin{aligned} \rho_0^{\mathrm{up/down}} &= \left[1.46k^2 \int_0^z dh \left(1 - \frac{h}{z}\right)^{\frac{5}{3}} \gamma_{(h)}^{\mathrm{up/down}}\right]^{-\frac{3}{5}}, \\ \gamma_{(h)}^{\mathrm{up}} &= C_n^2(h), \\ \gamma_{(h)}^{\mathrm{down}} &= C_n^2(z-h) \end{aligned} \tag{3.11}$$

which can be used to determine the amount of beam spread induced by turbulence. For example, a Gaussian beam with an initial beam waist of 15 cm, a wavelength of 800 nm, propagating from a 500 km satellite at zenith will have a diffraction-induced beam waist of 86.2 cm. The spatial coherence is calculated using equation 3.11 to be 9.1723 m. When this is subbed into equation 3.10, the square root of the answer determines the total beam spread to be 86.22 cm, indicating a 0.02 cm spread induced by turbulence. For the same conditions, a 1550 nm beam will have a final spot size of 1.6515 m with 1.6514 m resulting from free space diffraction. At 4

μm, there is no difference between the vacuum propagation beam spot size and the turbulent propagation beam spot size. These equations work as long as the number of turbulence-induced short-term speckles remain close to unity.

$$N_s = 1 + (a_R/\rho_0)^2 \tag{3.12}$$

Pirandola notes that for N_s to remain close to 1, the receiver aperture radius a_r must be kept below 2 m [40]. However, as the wavelength increases, the spherical coherence increases significantly, enabling larger apertures to be used while keeping N_s close to unity.

As previously mentioned, the spatial filtering technique described in [52] is utilized to permit daytime operation. Although the free space beam spread can be considered negligible, the authors use the Strehl ratio S, to account for the reduced spatial coherence at the receiver entrance pupil which leads to a broadened spot size in the focal plane [52]. The Strehl ratio is a measure of the quality of an optical system or of the image it produces. In the case of turbulence, the Strehl ratio compares the aberrated wavefront to an ideal aberration-free wavefront. In this work, the Strehl ratio is used as a way to represent the wavefront changes that occur as the strength of turbulence is varied.

$$S = \left[1 + \left(\frac{D_{\mathrm{R}}}{r(\lambda)}\right)^{5/3}\right]^{-6/5} \tag{3.13}$$

where $r(\lambda)$ is the coherence length given by [52]

$$r(\lambda) = r_0\left(\frac{\lambda}{\lambda_0}\right)^{6/5} \tag{3.14}$$

Here r_0 is the coherence length measured at $\lambda_0 = 500$ nm and is inversely related to the strength of turbulence. r_0 can be considered a wavelength-independent description of the turbulence strength.

Adaptive Optics (AO) systems utilize a deformable mirror to correct turbulence-induced wavefront aberrations and have been shown to significantly improve the performance of QKD systems operating in a turbulent channel [100][101][102]. Following the work in reference [52], a 200 Hz closed-loop bandwidth AO system is adopted which yields an effective $r_0 \approx 50$ cm [52]. Thus using the Strehl ratio and r_0, the effect of turbulence can be adjusted to emulate the operation of an adaptive optics system without the computational intensity of phase screen modelling and subsequent aberration corrections.

3.2 Quantum Communication

Quantum key distribution (QKD) was first proposed in the 1970's and is now perhaps the most mature quantum technology, being commercially available for over 17 years. In contrast to classical cryptography, quantum key distribution protocols use the principles of quantum mechanics to provide an unconditionally secure way to share encryption keys. These protocols can even detect the presence of an eavesdropper in the system who is attempting to intercept the key. To understand how this is possible, some key concepts are introduced.

Polarization:
Polarization is a property used to specify the geometrical orientation of the oscillations of a transverse electromagnetic wave. Light waves are electromagnetic waves which consist of coupled oscillating electric and magnetic fields that are perpendicular to each other [22]. Polarization in the context of light waves refers to the direction of the electric field, purely by convection. Most sources of radiation, including the sun, transmit light waves whose electric field oscillates in all perpendicular planes with respect to the direction of propagation. However, a polarization filter can be used to restrict light to a single plane where all waves oscillate in the same plane. Light waves can be linearly polarized, where the fields oscillate in a single direction or circularly polarized, where the fields rotate at a constant rate in a particular plane as the wave travels. Linearly polarized light can be vertically, horizontally or diagonally polarized.

Heisenberg's Uncertainty Principle:
Heisenberg's Uncertainty Principle states that in a quantum system only one property of a pair of conjugate properties can be known with certainty. Heisenberg, who was initially referring to the position and momentum of a particle, described how any conceivable measurement of a particle's position would disturbs its conjugate property, the momentum. It is therefore impossible to simultaneously know both properties with certainty. Quantum cryptography leverages this principle and generally uses the polarization of photons on different bases as the conjugate properties in question [4].

The No Cloning Theorem:
The No Cloning Theorem follows from Heisenberg's Uncertainty Principle and states that it is impossible to create identical copies of an unknown quantum state [22]. This makes it possible to find out if an eavesdropper interrupted the quantum channel during key transmission.

Dirac Notation:
Dirac notation is a widely used notation which can be used to express quantum mechanical relationships extremely efficiently [21][22][4]. Dirac notation works because the state of a quantum system can be expressed as a vector in an associated Hilbert space [22] which makes it easy to distinguish between scalars, vectors, and operators. By representing the wave function

Notation	Description
z^*	Complex conjugate of the complex number z. $(1+i)^* = 1-i$
$\|\psi\rangle$	Vector. Also known as a ket.
$\langle\psi\|$	Vector dual to $\|\psi\rangle$. Also known as a bra.
$\langle\varphi \mid \psi\rangle$	Inner product between the vectors $\|\varphi\rangle$ and $\|\psi\rangle$.
$\|\varphi\rangle \otimes \|\psi\rangle$	Tensor product of $\|\varphi\rangle$ and $\|\psi\rangle$.
$\|\varphi\rangle\|\psi\rangle$	Abbreviated notation for tensor product of $\|\varphi\rangle$ and $\|\psi\rangle$.
A^*	Complex conjugate of the A matrix.
A^T	Transpose of the A matrix.
$A^\dagger$	Hermitian conjugate or adjoint of the A matrix, $A^\dagger = \left(A^T\right)^*$. $\begin{bmatrix} a & b \\ & c \end{bmatrix}^\dagger = \begin{bmatrix} a^* & c^* \\ b^* & d^* \end{bmatrix}.$
$\langle\varphi\|A\|\psi\rangle$	Inner product between $\|\varphi\rangle$ and $A\|\psi\rangle$. Equivalently, inner product between $A^\dagger\|\varphi\rangle$ and $\|\psi\rangle$.

Table 3.1: Summary of Dirac notation.

as a vector and a physical observable as an operator then their interaction would be described by their inner product and will be an eigenvalue of the corresponding operator. This is where the Bra-Ket notation comes from. The conventions used in Dirac notation are extracted from reference [4] and shown in Table 3.1.

Qubits:

The fundamental concept of classical information and classical computation is the bit, which is simply a two-state system where the two states are referred to as 0 and 1 [21]. Quantum information theory has its own analogous concept, a basic element called the quantum bit, also known as a qubit [4]. A qubit is a quantum system with two orthonormal basis states $|0\rangle\, and\, |1\rangle$ which is represented using Dirac notation [4].

Superposition:

The fundamental difference between a classical bit and a qubit is the ability of the qubit to assume states other than 1 or 0. In addition, there is a possibility for a qubit to form a linear combination of states which are called superpositions and are denoted by $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ where the coefficients α and β are complex numbers [4]. The state of a qubit is represented as a vector in a two-dimensional Hilbert Space [4] where the computational basis states $|0\rangle\, and\, |1\rangle$ form an orthonormal basis for this space [22].

Entanglement:

Quantum entanglement is a physical phenomenon describing two or more particles in such a way that each particle's quantum state cannot be described independently of the state of the other particles, even if the particles are separated by a large distance [103]. When two entangled particles are released from a source, they exhibit highly correlated characteristics which are kept even when they move away from each other. A measurement of the state of one particle changes the state of the other entangled particles immediately.

Physical Observables and Hermitian Operators:
A physical observable is anything that can be measured. In quantum mechanics, to each physical observable, there is a corresponding operator. The eigenvalues of the corresponding operator will always be real making the operator Hermitian. An operator A is said to be Hermitian if it is equal to its adjoint, $A = A^{\dagger}$ [4]. An observer is therefore a linear operator such that if the observable Ω is applied to the state vector $|\psi\rangle$ then the resulting state will be $\Omega\,|\psi\rangle$. The only possible values that observables can take are the eigenvalues of the Hermitian operator. The eigenvectors of this Hermitian operator form the basis for the state space [21].

Measurement:
In quantum mechanics, measuring is the act of carrying out an observation on a physical system. It is a process that involves asking the system a specific question and receiving an answer [21]. If Ω is an observable and $|\psi\rangle$ is a state, then the result of measuring Ω is given by the eigenvalue λ and the resulting state after the measurement will always be an eigenvector $|\lambda\rangle$ that corresponds to λ [21]. The probability of $|\psi\rangle$ collapsing into an eigenvector $|\lambda\rangle$ is given by the length squared of the projection of $|\psi\rangle$ onto $|\lambda\rangle$. Such that the probability of getting the eigenvector $|\lambda\rangle$ when measuring the state $|\psi\rangle$ will be $|\,\langle\lambda|\psi\rangle\,|^2$. When a measurement is made, the wave function will collapse to a given eigenvector, making the act of measuring an irreversible process. Therefore when several observables are measured, the order of the measurements matters [21].

Quantum Key Distribution:
Quantum key distribution exploits the nature of quantum mechanics to enable provably secure communication between two parties, usually referred to as Alice and Bob. Although any quantum state can be used as an information carrier, in almost all cases photons are used due to their high speed and low decoherence relative to alternative quantum states. Although Continuous-Variable QKD has seen rapid development in recent years, most QKD protocols are Discrete-Variable algorithms based on the polarization states of photons. Generally, QKD protocols achieve secure key exchange by executing the following steps; raw key exchange, key sifting and classical post-processing [103]. Raw key exchange refers to the process where the quantum states are created and transmitted over a quantum channel to generate a cryptographic key. Next, a "sifted key" is extracted from the raw key based on some selection process which differs between protocols. Finally, classical error correction and privacy amplification techniques are utilized to eliminate errors and detect the presence of Eve, an eavesdropper. If the Quantum Bit Error Rate (QBER) is above the security threshold, Alice and Bob will share the same secret key. It is important to note that Alice and Bob must share an authenticated classical communication channel [103].

3.2.1 BB84

The BB84 protocol is one of the most prominent QKD protocols and was proposed in 1984 by Bennett and Brassard which is where it gets its name [6]. Its security is based on the Heisenberg Uncertainty Principle and the no-cloning theorem. In this protocol, information is encoded into the polarization state of single-photons. For example, the transmitter, Alice, could use the rectilinear basis by encoding zeros into horizontally polarised photons and ones into vertically polarized photons, or vice versa. She can also encode zeros and ones using the diagonally polarized basis. The trick is to send out a sequence of polarized photons where the type of polarization used is selected randomly [104]. The receiver, Bob, measures the polarisation of these photons by randomly selecting a polarization basis to measure in. After a certain number of bits has been transmitted, Bob uses a classical authenticated channel to announce which basis he used for each bit. Alice then says in which cases they used the same bases. They throw out the bits where they used different bases, and leave only those where they used the same one. The no-cloning theorem guarantees that Eve cannot measure these photons and transmit them to Bob without disturbing the photon's state in a detectable way. To check for the presence of eve, Bob and Alice compare a section of the key for errors [104]. This occurs on a public channel so if no errors are detected, that section of the key is discarded and the remaining bits form the secret key. If they detect the presence of Eve, then the whole key is discarded and the procedure is repeated again until a secret key can be generated [104].

The BB84 protocol is ideally implemented using a single-photon source but attenuated laser pulses (weak coherent states) are commonly used in real-world QKD systems, and they occasionally emit more than one photon. This makes the system vulnerable to sophisticated eavesdropping attacks [14][15][16]. Photon number splitting (PNS) attacks are one of the most widely discussed eavesdropping techniques in which Eve intercepts all single-photon signals and splits multi-photon signals, storing one photon in a quantum memory and sending the rest to Bob. During the sifting process, Eve can observe the classical communication channel to determine which basis states were used by bob, and measure the stored photons accordingly. If Eve gathers sufficient information then the security of the key exchange is compromised. The decoy-state method was proposed by Hwang [17] to overcome this vulnerability.

3.2.2 Decoy-state Method

Given a weak coherent state, the number of photons in each pulse follows a Poisson distribution where the average photon number μ is set by Alice. The density matrix of this state is given by

$$\rho_A = \sum_{i=0}^{\infty} \frac{\mu^i}{i!} e^{-\mu} |i\rangle\langle i| \tag{3.15}$$

where $|0\rangle\langle 0|$ is the Dirac notation representation of the vacuum state and $|i\rangle\langle i|$ is the Dirac notation density matrix of the i-photon state when $i = 1, 2..$ [105]. As a result, there is a nonzero chance that each light pulse contains more than one photon which exposes the protocol to PNS attacks. During a PNS attack, Eve selects subsets of multi-photons to transport to Bob. Typically Eve is assumed to possess infinite computational and technological power so her communication channel with Bob is presumed to be lossless. As a result, the yield of pulses transmitted by Eve will be significantly higher than the yield of pulses sent via Alice's lossy channel. The basic idea of the decoy-state method is for Alice to transmit two different signals, the typical BB84 signal states used to generate the key and the decoy-states, which are used to identify the presence of Eve. Alice randomly modulates the intensity of the coherent states which results in varying photon number statistics across the channel. Eve can't tell the difference between multi-photon pulses originating from signal or decoy states. As a result, the normalized yield of multi-photon pulses are expected to be similar for decoy and signal states. Once Bob receives the photons, Alice announces which pulses were decoy states and through a public discussion, they determine the total yield of the decoy states and that of the signal states. If the yield of the decoy-states is much larger than the yield of the signal-states, then the whole protocol is aborted. Note that the difference in mean photon number between the signal states and the decoy states plays a crucial role in enhancing the security and estimating the channel loss. The signal states serve as the primary states for transmitting the quantum information during the key distribution process, carrying the actual secret key between the sender and the receiver.

To enhance the security, signal states with different mean photon numbers are used, including both low-intensity and high-intensity signal states. Low-intensity signal states have a low mean photon number and are typically generated using weak coherent pulses. They are more vulnerable to losses and certain eavesdropping strategies due to their lower photon count. However, they offer advantages in terms of security as they are less likely to be intercepted without detection. High-intensity signal states have a higher mean photon number and are typically generated using strong coherent pulses. They have a higher photon count and can withstand losses better but are also more susceptible to certain eavesdropping strategies. In contrast, the decoy states have specific mean photon numbers that differ from the mean photon numbers of the signal states. Decoy states are used in this protocol for two main purposes, estimation of channel loss and detection of eavesdropping attempts. By comparing the detection rates of the decoy states with different mean photon numbers at the receiver's end, it becomes possible to estimate the loss experienced by the quantum channel. The detection rates of the decoy states serve as reference values, allowing for the determination of the channel's characteristics and potential losses. Equally as important, decoy states with known mean photon numbers also aid in detecting eavesdropping attempts, where any inconsistency between the expected detection rates and the measured detection rates suggests the presence of an eavesdropper.

The security of the channel can be determined if Alice and Bob estimate the yield and QBER for the signal-states and decoy-states. The yield for a given state Y_i, is the conditional probability that Bob detects the transmitted state if i-photons are sent by Alice [106]. The QBER for a given state e_i, is the ratio between the erroneous bit probability and the probability of successful bit transmission, when i-photons are sent by Alice [106]. Y_i and e_i are easily determined for the case of infinite decoy states. Y_i is a combination of the background noise and the signal so Y_i can be written as [105]

$$\begin{aligned} Y_i &= Y_0 + \eta_i - Y_0\eta_i \\ &\cong Y_0 + \eta_i. \end{aligned} \tag{3.16}$$

where n_i is the transmittance of i-photon states. The corresponding gain of i-photon states is a combination of the i-photon yield Y_i and the Poisson distribution probability of Alice sending an i-photon state. The i-photon state gain Q_i is given by [105]

$$Q_i = Y_i \frac{\mu^i}{i!} e^{-\mu} \tag{3.17}$$

The Quantum Bit Error Rate for an i-photon state e_i is given as [105]

$$e_i = \frac{e_0 Y_0 + e_{\text{detector}}\, \eta_i}{Y_i} \tag{3.18}$$

where e_0 is the random background error rate and $e_{detector}$ is the probability that a photon hits the detector. The overall gain is determined by summing the individual gain parameters for each i-photon state

$$\begin{aligned} Q_\mu &= \sum_{i=0}^{\infty} Y_i \frac{\mu^i}{i!} e^{-\mu} \\ &= Y_0 + 1 - e^{-\eta\mu} \end{aligned} \tag{3.19}$$

Finally the overall QBER E_μ for pulses with intensity μ is

$$\begin{aligned} E_\mu Q_\mu &= \sum_{i=0}^{\infty} e_i Y_i \frac{\mu^i}{i!} e^{-\mu} \\ &= e_0 Y_0 + e_{\text{detector}} \left(1 - e^{-\eta\mu}\right). \end{aligned} \tag{3.20}$$

So when infinite decoy states are utilised, Y_i and e_i are easily determined. However, in [105] they demonstrate using only two types of decoy states, vacuum and a weak decoy-state, that the attained key rate is very close to that achieved using an infinite number of decoy states. In this scenario the source emits either signal states with average photon number μ, decoy vacuum states or decoy coherent pulses where the mean photon number (MPN) ν is less than the MPN of the signal-state i.e. $\nu < \mu$. The secure key generation rate per use is given by [105]

$$R \geq q\left\{-Q_\mu f\left(E_\mu\right) H_2\left(E_\mu\right) + Q_1\left[1 - H_2\left(e_1\right)\right]\right\} \tag{3.21}$$

where q is the protocol efficiency, Q_1 is the signal-state gain, e_1 is the single-photon state error rate, $f(E_\mu)$ is the bidirectional error correction efficiency and H_2 is the Shannon binary entropy function defined as [105]

$$H_2(x) = -x \log_2(x) - (1-x)\log_2(1-x) \tag{3.22}$$

3.3 Signal to Noise Ratio

Following the theoretical description of the phenomena affecting the channel, the following sections seek to characterise the channel be defining two principal metrics, signal to noise ratio (SNR) and secret key rate (R). Here the losses resulting from diffraction, absorption, scattering, excess noise and turbulence-induced wavefront errors are used to determine these metrics. The signal to noise ratio is a useful metric for quantifying the quality of the channel, it compares the signal that reaches the detector to the noise that reaches the detector. To determine the signal to noise ratio, the signal gain and background probability must be calculated.

3.3.1 Background Probability

The background probability Y_0 is the probability that the detector measures a non signal photon and is calculated by combining the number of sky photons entering the detector N_b, with the detector dark count rate f_{dark}

$$Y_0 = N_b\, \eta_{det}\, \eta_{opt} + 4 f_{dark}\, \Delta t \tag{3.23}$$

where η_{opt} is the overall efficiency of the optical setup at the receiver including the spectral filter efficiency and η_{det} is the detector efficiency. Although the background probability is dominated by N_b, a number of filtering techniques can be utilized to reduce the background probability and improve the signal to noise ratio and ultimately the secret key rate. Three such methods are described in [107] and each is incorporated into this study.

Temporal Filter

A narrow temporal filter temporarily opens to allow signal photons through to the detector and closes once the signal has passed, blocking out the remaining noise photons. Precise synchronization is required to effectively block out noise and as such a practical filter of 1 ns is chosen.

Spectral Filter

A number of light sources contribute to the accumulated background noise including solar, lunar and terrestrial radiance, which results in a spectrum of continuous wavelength noise. Much of this noise can be blocked by using a narrow spectral filter which selectively allows light of certain wavelengths to pass through. A 1 nm spectral filter is used.

Spatial Filter

Two spatial filtering strategies are proposed in [52], a diffraction limited (DL) strategy and a turbulence limited (TL) strategy. The key difference between the strategies is whether the field stop grows to accommodate the turbulence broadened beam spot (TL) or remains constant at the diffraction limit (DL). The authors show how the turbulence limited strategy predicts higher secret key rates for a number of site conditions. Thus here we adopt the turbulence limited strategy in which the size of the field stop is varied to always allow 84% of the signal through. The choice of spatial filter determines the solid-angle field of view (FOV) which is given by:

$$\Omega_{FOV} = \pi \left(1.22 \, \frac{\lambda}{D_r} \left[1 + \left(\frac{D_r}{r(\lambda)} \right)^{5/3} \right]^{3/5} \right)^2 \tag{3.24}$$

Notice that the Ω_{FOV} rises quadratically with wavelength, which makes spatial filtering significantly more effective at shorter wavelengths. For a given temporal filter Δt, spectral filter $\Delta\lambda$ and spatial filter field of view Ω_{FOV}, the number of sky noise photons, N_b, entering the receiver is described by the radiometric expression [108]

$$N_b = \frac{H_b \Omega_{FOV} \pi D_r^2 \lambda \Delta\lambda \Delta t}{4hc} \tag{3.25}$$

where H_b is the spectral radiance calculated using MODTRAN, h is Planck's constant and c is the speed of light. Note that the number of noise photons is proportional to the wavelength, radiance, FOV, receiver size and filter size. If the radiance is constant at different wavelengths, then the number of noise photons is proportional to wavelength and thus favours shorter wavelengths. However, radiance is not constant and is highly dependent on both wavelength and site conditions.

3.3.2 Channel Efficiency and Signal Gain

Now that the background probability has been defined, the channel efficiency can be derived and used to determine the signal to noise ratio. The total channel efficiency is calculated by taking the product of each loss factor.

$$\eta = \eta_d \, \eta_{trans} \, \eta_{FS} \, \eta_{opt} \, \eta_{det} \tag{3.26}$$

where η_d is the diffraction-induced beam spread loss, η_{trans} is the absorption and scattering losses, η_{det} is the detector efficiency and η_{FS} is the field stop loss, set to 0.84 for the turbulence limited strategy. The decoy-state protocol signal to noise ratio is used to evaluate the performance of the channel and is as defined in [105]:

$$SNR = Q_n/Y_0 \tag{3.27}$$

where Q_n is the signal-state or decoy-state gain given by:

$$Q_n = Y_0 + 1 - e^{-\eta n} \tag{3.28}$$

and n is mean photon number (MPN) of the signal-state (μ) or decoy-state (ν). Although some previous implementations used relatively low MPN values [105][101], advances in detector technology permit better performance using higher optimal values [52] [109]. In this work, the chosen values for the signal and decoy-state MPNs are $\mu = 0.7$ and $\nu = 0.1$ respectively.

3.4 Secret Key Rate

To fulfil the purpose of this thesis, a decoy-state BB84 QKD protocol is implemented and used as a performance metric to identify what wavelengths are available for satellite downlink quantum communication. Ideally, this protocol is implemented using a single-photon source but as already mentioned in practical implementations, attenuated laser pulses (weak coherent states) are commonly used, and they occasionally emit more than one photon which makes them vulnerable to PNS attacks. To avoid this security flaw, the decoy-state BB84 protocol is utilized, using only vacuum and weak decoy-states. Recall from equation 3.21 that the secret key generation rate per signal-state for the decoy method BB84 protocol can be expressed as

$$R \geq q\left\{-Q_\mu f\left(E_\mu\right) H_2\left(E_\mu\right) + Q_1\left[1 - H_2\left(e_1\right)\right]\right\}$$

where the protocol efficiency q is 1/2 for the BB84 protocol because on average Alice and Bob choose the same basis half of the time, f_{ec} is the error correction efficiency set as 1.22, a commonly used value associated with cascade error correction [101] and $H_2(x)$ is the Shanon binary entropy formula defined in equation 3.21. The decoy/signal quantum bit error rate (QBER) is given in equation 3.20 and when the formulas for n_i and Y_i are subbed in, the QBER can be rewritten as

$$E_{\mathrm{r},n} = \frac{e_0 Y_0 + e_{\mathrm{d}}\left(1 - e^{-\eta n}\right)}{Y_0 + 1 - e^{-\eta n}} \tag{3.29}$$

where the background error rate $e_0 = 0.5$ for randomly occurring dark and background counts and the polarization cross-talk error $e_d = 0.01$. The single-photon gain can be defined as [105]

$$Q_1 = \frac{\mu^2 e^{-\mu}}{\mu\nu - \nu^2}\Big(Q_\nu e^\nu - Q_\mu e^\mu \frac{\nu^2}{\mu^2} - \frac{\mu^2 - \nu^2}{\mu^2} Y_0\Big) \tag{3.30}$$

The single-photon yield is defined by [105]

$$Y_1 = \frac{\mu}{\mu\nu - \nu^2}\left(Q_\nu e^\nu - Q_\mu e^\mu \frac{\nu^2}{\mu^2} - \frac{\mu^2 - \nu^2}{\mu^2} Y_0\right) \tag{3.31}$$

Finally, the single-photon state error rate is given by [105]

$$e_1 = \frac{E_{\mathrm{r},\nu} Q_\nu e^\nu}{Y_1 \nu} - \frac{e_0 Y_0\left(\lambda\right)}{Y_1 \nu} \tag{3.32}$$

Fig. 3.9 shows the flow of information around the channel model and provides some insight into the relationship between the parameters and the functions that act on them. The model is initialized with the scenario parameters including geometric, geographic and atmospheric information about the channel. MODTRAN uses these inputs to determine the atmospheric extinction and spectral radiance for the chosen scenario. The MODTRAN output now acts as an input to the rest of the model, enabling calculations of channel efficiency and background probability which are then used to determine the signal/deocy state gain and quantum bit error rate (QBER). Finally the secret key rate can be calculated and analysed to determine the most suitable wavelengths for the chosen scenario. Secret key rate surface plots are used throughout this thesis to show how performance varies as a function of λ, D_r and w_0.

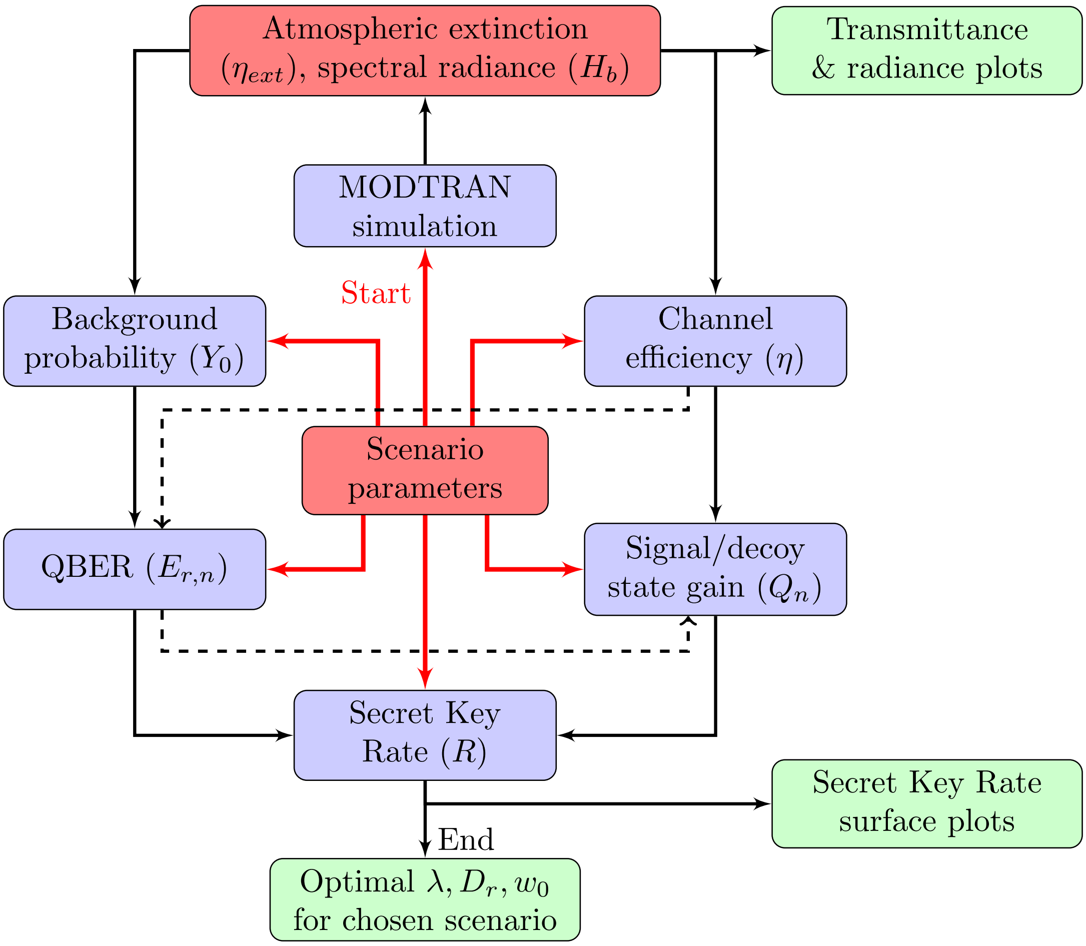

Atmospheric extinction (η_{ext}), spectral radiance (H_b)
Transmittance & radiance plots
MODTRAN simulation
Start
Background probability (Y_0)
Channel efficiency (η)
Scenario parameters
QBER ($E_{r,n}$)
Signal/decoy state gain (Q_n)
Secret Key Rate (R)
Secret Key Rate surface plots
End
Optimal λ, D_r, w_0 for chosen scenario

Figure 3.9: Flow diagram showing the flow of information through the channel model where the inputs are red, the algorithms and functions are blue and the outputs are green.

In this chapter, the relevant theory necessary to understand this thesis was briefly summarised and the channel model was described. In the following chapters, this model is used to analyse the performance of the satellite downlink channel and determine which wavelengths are suitable for real world quantum satellite communications.

Chapter 4

Results, Analysis and Discussion

In this chapter, the results of this thesis are presented, analysed and discussed. The goal of this research is restated here to clarify the intention of the work and to give context to the results. The main aim of this research is to find the most suitable wavelengths for quantum key distribution in the satellite downlink channel, while operating in daylight under realistic and adverse atmospheric conditions. This chapter is broken down into the following sections. First, the atmospheric extinction and spectral radiance are investigated across a wide range of wavelengths, from 400 nm in the visible window to 12 μm in the LWIR window. Each wavelength is separated into channels based on the size of the spectral filter used by the receiver. For each channel, the signal to noise ratio and the secret key rate is calculated and compared to find the best channels. The component sizes are also varied and used to find the most applicable wavelengths for practical QKD, due to the effect that the transmitter and receiver size have on wavelength selection and secret key rate optimization. The analysis begins by identifying the wavelength-receiver pair that produces the highest secret key rate. The best wavelengths are selected from each window and used to represent their respective regions in a comparison. This serves to give an example of what is possible in terms of QKD. However, for practical QKD there is often a limit on receiver and transmitter sizes so the best wavelengths for each component size is shown. This section concludes by comparing the performance of each transmission window in the presence of adverse weather conditions such as fog, haze and rain.

4.1 Atmospheric Extinction and Spectral Radiance

Wavelength selection for classical communications is relatively straightforward in comparison to quantum communications. A classical communication system seeks to optimise signal to noise ratio which makes the wavelength selection process simplistic. Wavelengths that maximise transmission and minimise excess noise will be good candidates. However, as this chapter progresses, the methodology for selecting wavelengths to optimise the secret key rate for quantum communications is not so easy. In this section, we analyse some of the most important parameters which determine both signal to noise ratio and secret key rate. Specifically, we analyse wavelength selection by calculating the absorption and scattering due to the gaseous structure of earth's atmosphere. This allows the percentage transmission for each wavelength to be determined, as they propagate from a satellite down through earth's atmosphere. Additionally, the spectral radiance is calculated by combining radiation emitted from a number of bodies including the sun, the moon and the earth itself. Thus between the transmission and radiance at the ground receiver, a crude estimate of signal to noise ratio can be estimated. MODTRAN, which was described in detail in the methodology section, is used here to simulate the propagation of light of varying wavelengths as they move down through the atmosphere. The atmospheric generation toolkit is used to generate the atmosphere, so that location-specific data can be extracted.

4.1.1 Scenarios

One of the most important and often overlooked aspects of practical QKD is the availability of the system. As research in this field transitions from feasibility studies to practical implementation and optimization studies, availability will become a key point of discussion. Furthermore, if FSOC QKD is to help establish the quantum internet and truly democratise the power of quantum technologies, these systems must yield secret key rates in a variety of atmospheric conditions and geographical locations.

Two very different scenarios are considered, the clear skies of Tucson, Arizona are compared with the wet and cloudy climate of Waterford, Ireland. MODTRAN is used to simulate these atmospheres and determine the transmission and spectral radiance across a range of wavelengths. Spectral radiance is highly dependent on the sun's position in the sky relative to the earth and as such a specific-location and time must be specified.

Tucson, Arizona
At noon on the summer solstice (June 21^{st}), the desert climate of Tucson experiences wind speeds of 3.33 m/s [110] with desert aerosols and albedos. The visibility is set to 70 km to represent a clear sky. The transmittance (green) and spectral radiance (block) for a ground receiver pointed at zenith is plotted across the electromagnetic spectrum and shown in Figure 4.1.

Waterford, Ireland
In contrast, at noon on the winter solstice (December 21^{st}), the Irish coastal region of Waterford typically experiences rural aerosols with visibilities of 23 km and farm albedos. Similarly, the transmittance (blue) and spectral radiance (red) is also plotted in Figure 4.1 for direct comparison with data from Tucson. At this time of year Waterford is often plagued by clouds [111], here a cirrus cloud model is used but later more opaque variants typically seen in Waterford are considered. While Tucson represents an ideal location for satellite communications, the wet and cloudy skies of Waterford represent regions where satellite communications are more challenging. The transmission and spectral radiance data are extracted from MODTARN as json files and imported into MATLAB. The resolution in MODTRAN is limited by the length of the longest wavelength being modelled. For this reason, the full spectrum is modelled and plotted purely for visual comparison as shown in Figure 4.1. To accurately determine the best wavelengths, the spectrum is broken down into transmission windows. The regions considered throughout this work are as follows:

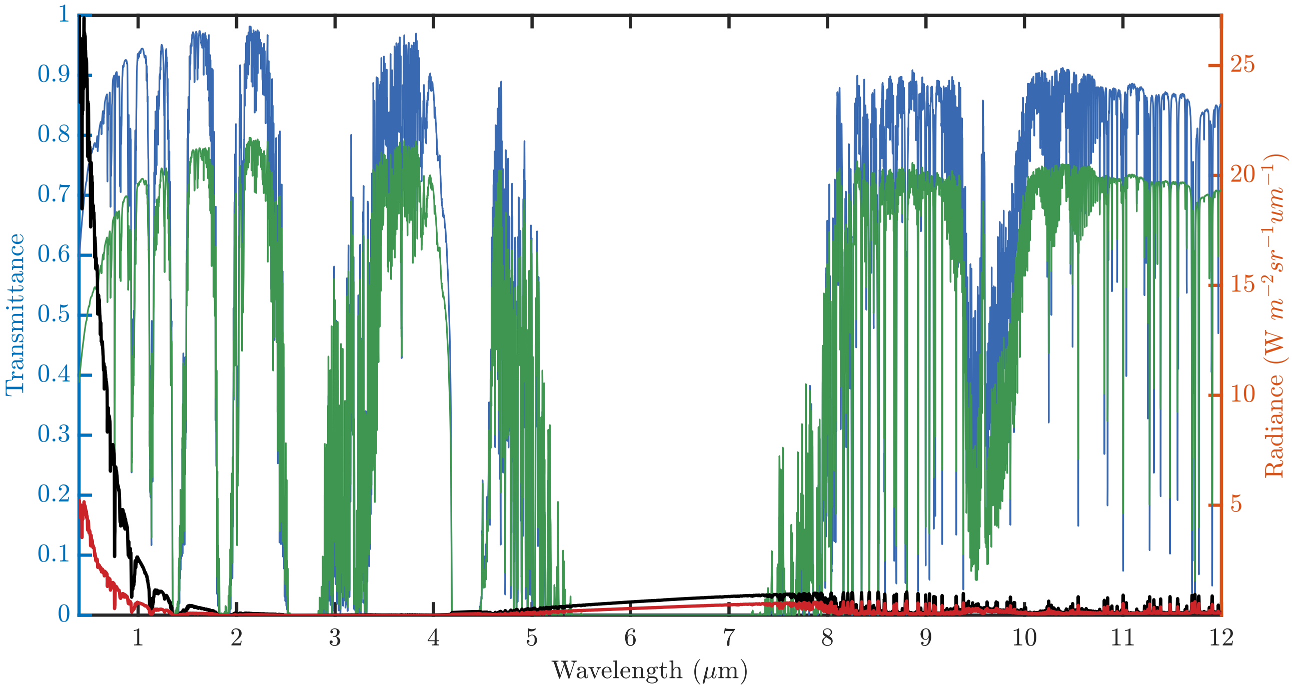
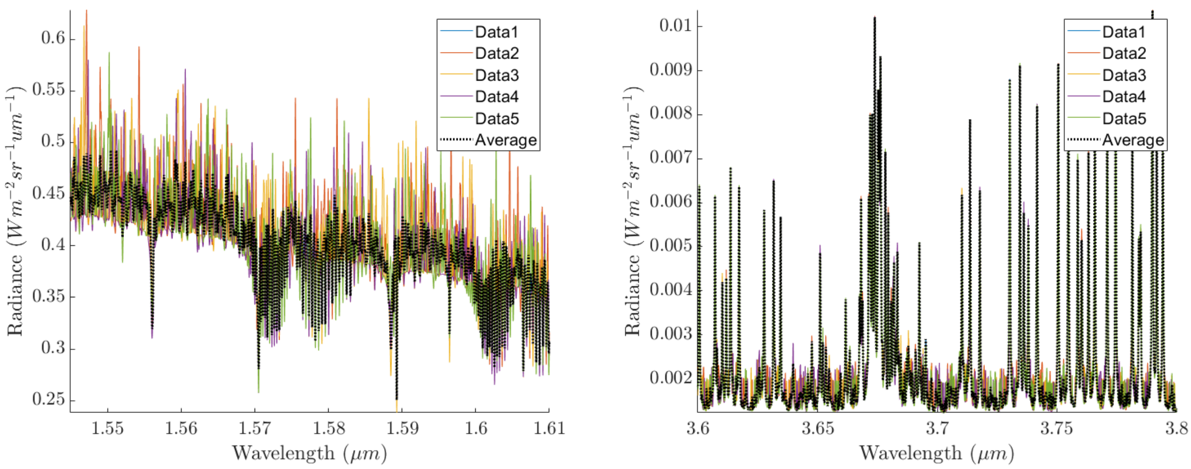


Figure 4.1: Transmittance and radiance plotted as a function of wavelength in Waterford and Tucson. The Transmittance and radiance in Waterford are coloured green and red respectively while blue and black are used to represent the equivalent data for Tucson.

- Visible 0.4 μm - 0.75 μm
- Near-infrared (NIR) 0.75 μm - 1.4 μm
- Short-wavelength infrared (SWIR) 1.4 - 3 μm
- Mid-wavelength infrared (MWIR) 3 - 8 μm
- Long-wavelength infrared (LWIR) 8 - 15 μm
- Far-infrared (FIR) 15 μm - 1 mm

As daily solar, lunar and terrestrial radiation in a given location is determined via a stochastic process [112], the total spectral radiance in MODTRAN follows some statistical distribution. To accurately determine the radiance, average values must be used to uncover the underlying distribution. This variance in spectral radiance is shown in Figure 4.2, for a) SWIR channel in Tucson and b) MWIR channel in Waterford. Five data sets represent five MODTRAN simulations which are shown using solid lines and labelled accordingly. The average radiance for each wavelength is taken and shown using a dotted black line. It is this new averaged data set that will be used to find the optimal channels. The MODTRAN generated transmission at each wavelength is largely deterministic so it remains the same for each data set. The new averaged radiance data corresponds to the average radiance at a specific wavelength. However, the QKD model used in this work is assisted by spatial and spectral filtering techniques, described in chapter 2. To this end, a spectral filter is used to ensure that signal wavelengths are received



(a) Tucson SWIR Channel 1

(b) Waterford MWIR Channel 1

Figure 4.2: Demonstrating the variance in spectral radiance for a)a SWIR channel in Tucson and b) a MWIR channel in Waterford. Five data sets represent five MODTRAN simulations which are shown using solid lines and labelled accordingly while the average is indicated by the dotted black line

while excess noise from the sun, moon and earth are blocked. In practice, the width of the spectral filter has to be large enough to let the signal through and in the process, other wavelengths can enter the receiver. Thus to properly determine the effect that radiance has on the system, the radiance must be averaged across the filter width. For example, most of the calculations in this work are done using a 1 nm spectral filter. An algorithm was designed to scan across each of the wavelengths in the dataset and create a channel centred on that wavelength, with a width of ± the spectral filter width/2. For example in the case of a 1 nm filter being applied to a centre wavelength of 780 nm, the newly created channel ranges from 779.5 nm to 780.5 nm. The transmission and radiance of this channel are an average of all the intermediate data points in that range. This gives a better indication of the radiance that will be received by the detector while also accounting for variances in the laser's source wavelength.

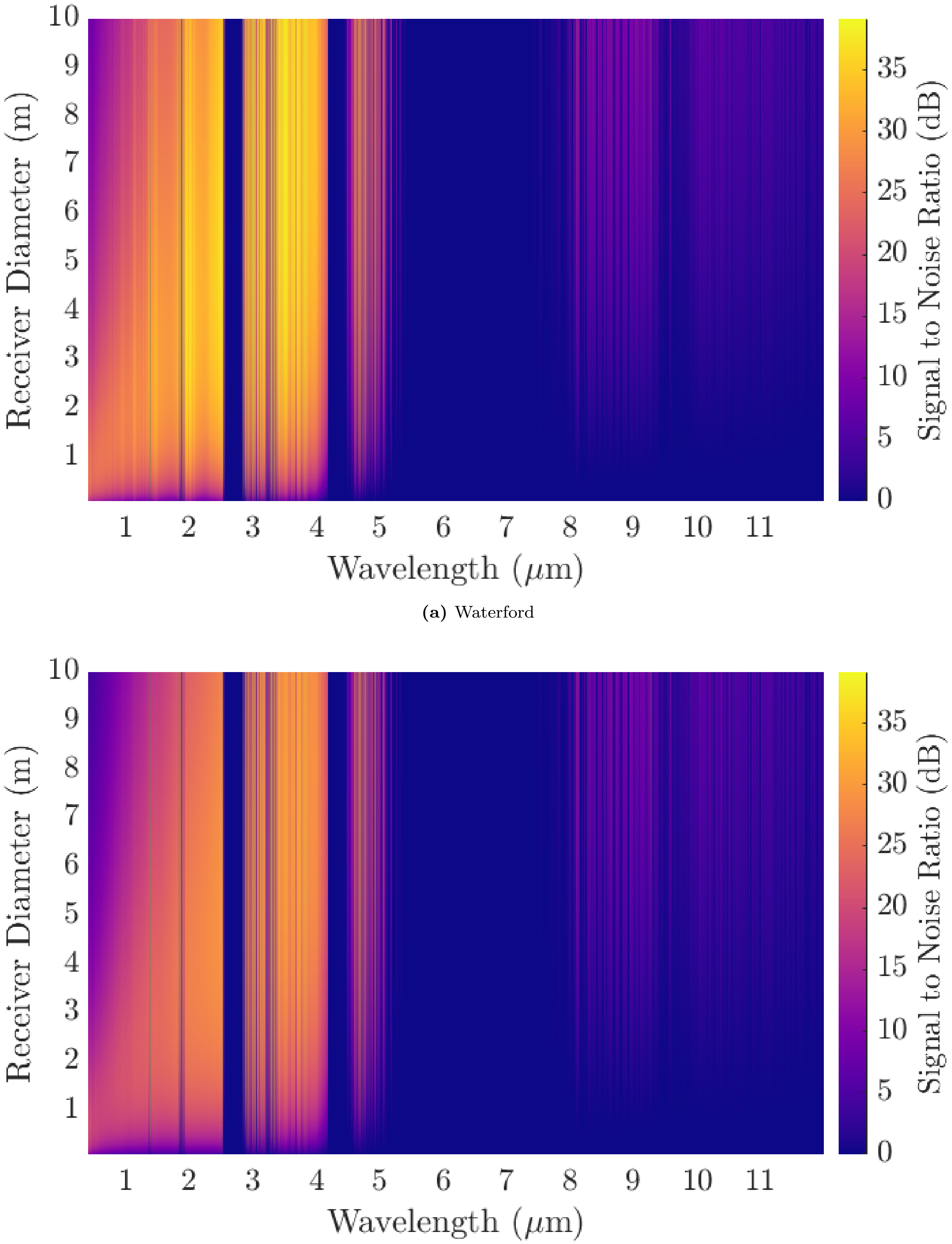
The new channels and their respective transmittance and radiance are stored as arrays to be further analysed in MATLAB. For each channel, the signal to noise ratio and secret key rate can be determined using the channel model and BB84 decoy-state protocol described in chapter 2. From here, one could plot wavelength against signal to noise ratio and secret key rate to determine the optimum wavelengths. However, there are a number of other important variables which must be considered. More detail is given on these variables later in this chapter, but for now, the signal to noise ratio is calculated as a function of wavelength and receiver size. Both of these parameters are critical in the design of any free-space optical communication system. The importance of wavelength on signal to noise ratio can be seen graphically in Figure 4.1 but the implications of the receiver size are less apparent. As the receiver size is increased, the channel efficiency is increased and so the signal gain is higher. At the same time, as the receiver size is increased the FOV of the receiver broadens and the number of noise photons that enter the system also increases. So it is not easy to say exactly how the signal to noise ratio will respond to a change in receiver diameter as the wavelength is also varied. The best way to understand the interaction between wavelength and receiver size and their combined effect on signal to noise ratio is to plot them together in a 3-dimensional graph. The following plots (Figure 4.3 and Figure 4.4) show surface plots with the centre wavelength on the x-axis, the receiver diameter on the y-axis and the signal to noise ratio on the z-axis. The SNR in dB is represented using a colourmap, where the scale is given by the colourbar. The decoy-state BB84 signal to noise ratio is calculated using equation 3.27 for a ground receiver located at a) Waterford and b) Tucson, from a 500 km altitude satellite pointed at zenith, where the initial beam waist is alternated between 10 cm and 35 cm, the coherence length r_0 is 50 cm to represent the corrected wavefront resulting from 200 Hz adaptive optics unit. These parameters are summarised in table 4.1. In Figure 4.3 the signal to noise ratio is plotted as a function of wavelength and receiver size for an initial beam waist of 10 cm, in Waterford and Tucson. The same graph is re-plotted in Figure 4.4 using an initial beam waist of 35 cm. The choice of these variables is discussed in greater detail below. There are a few important things to note about these graphs. Firstly, the SNR is given in dB, so a slight change in colour corresponds to a huge difference in signal to noise ratio. When the SNR is plotted before being converted to dB, most of the spectrum is black with some coloured pockets in the SWIR, while the MWIR is significantly coloured roughly around 3 - 4 μm. While there are many areas on the plot that do have a good SNR, using the colourmap measures each region relative to each other so the vast SNR advantage of the MWIR shadows the other wavelength regions. So the SNR is converted to dB as $SNR_{dB} = 10\ X\ log(SNR)$, resulting in a more even colour distribution. Note that each figure has its own colour scale, producing a simple visual comparison of both atmospheric

Name	Value
η_{opt}	0.45
η_{det}	0.8
μ	0.7
ν	0.1
f_{dark}	10 Hz
Δt	1 ns
$\Delta\lambda$	1 nm
z	500 km
r_0	50 cm

Table 4.1: Summary of the constants used throughout this work to calculate signal to noise ratio and secret key rate. η_{opt} is the overall efficiency of the optical setup at the receiver including the spectral filter efficiency, η_{det} is the detector efficiency, μ and ν are the MPN's of the signal-states and decoy-states respectively, f_{dark} is the detector dark count rate, Δt is the temporal filter size, $\Delta\lambda$ is the spectral filter size, z is the propagation distance and r_0 is the coherence length.

scenarios for a given initial beam waist, without comparing the effect of initial beam waist which is done separately later in this section.

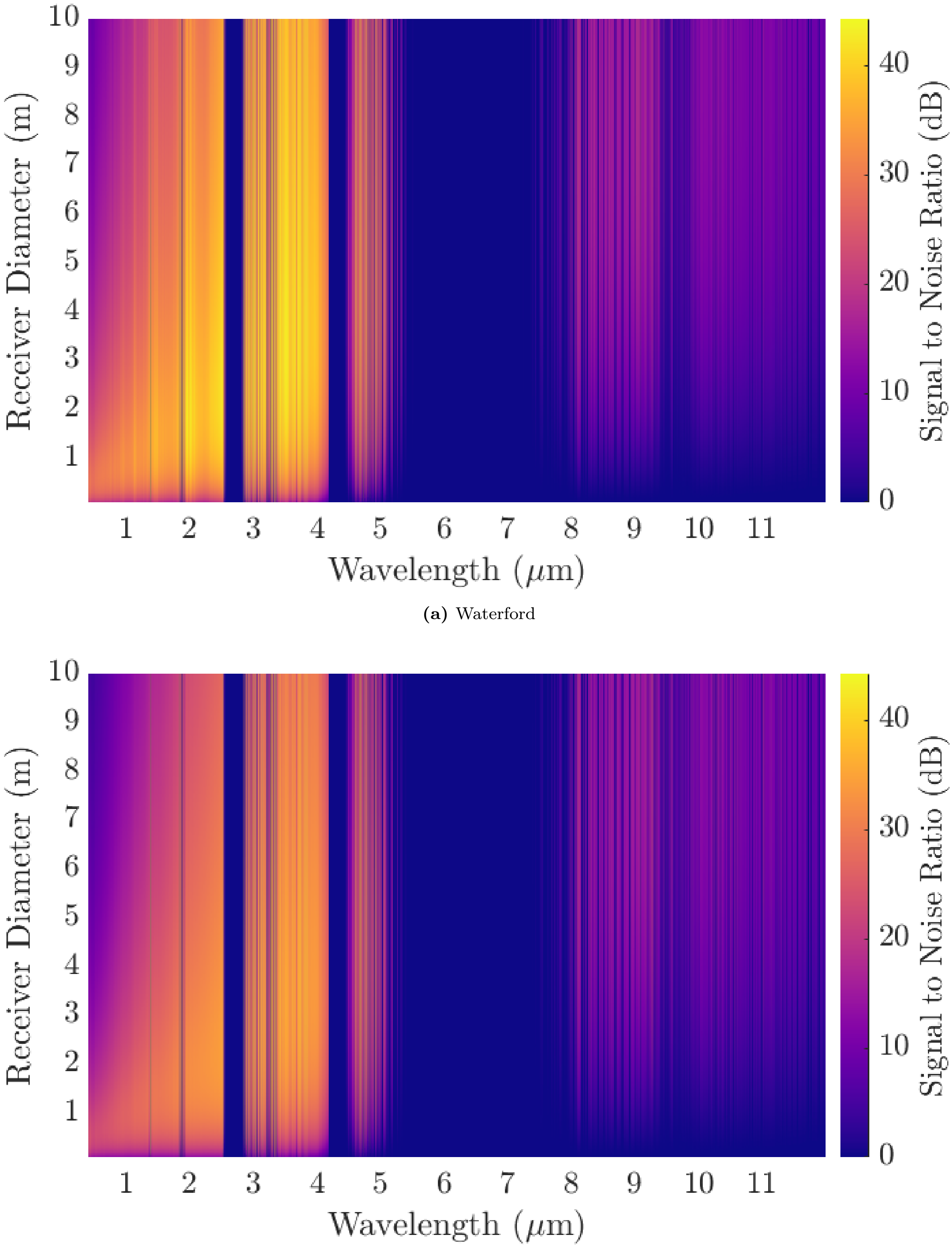
Interestingly, the SNR in Waterford is significantly higher than in Tucson, despite the absorption and scattering losses being much higher. This is due to a substantial reduction in solar radiance in Waterford relative to Tucson. This difference can be attributed to a number of different factors. Firstly, the Tucson data is compared on the summer solstice, at a time of day when the solar radiance peaks. In contrast, the atmosphere generated for Waterford, takes place on the winter solstice, again at a time of day corresponding to a peak in solar radiance. However, even when the simulations are run on the same days of the year, Tucson experiences significantly more solar radiation than Waterford due to its relative proximity to the sun. These factors combine to yield a meaningful difference in spectral radiance between the two considered scenarios which drives a considerable difference in the SNR achievable for a beam propagating through these two atmospheres. This is an important finding because taking a glance at Figure 4.1 seems to imply an advantage for Tucson, due to significant reduction in extinction loss. However, Figure 4.3 and Figure 4.4 highlight the influence that solar radiance has on the signal to noise ratio, and its importance for classical and quantum communications.



(a) Waterford

(b) Tucson

Figure 4.3: 3D surface plot representing the signal to noise ratio in a) Waterford and b) Tucson, for a range of receiver diameters and wavelengths when the initial beam waist is 10 cm and all other parameters are listed in table 4.1



(a) Waterford

(b) Tucson

Figure 4.4: 3D surface plot representing the signal to noise ratio in a) Waterford and b) Tucson, for a range of receiver diameters and wavelengths when the initial beam waist is 35 cm and all other parameters are listed in table 4.1

4.2 Wavelength Selection for QKD

When trying to maximise the performance of a QKD system, there are a number of parameters which must be optimised. To find what conditions permit the highest secret key rate, there is a key trade-off that must be considered. This trade-off is between signal gain and background noise and thus understanding both of these parameters is crucial for optimising the secret key rate.

The signal gain is ultimately determined by the channel efficiency, which is a multivariate equation given by 3.27. The overall efficiency is calculated as the product of the diffraction-induced free-space geometrical loss η_d, the atmospheric extinction loss η_{ext}, the field stop loss η_{FS}, the detector efficiency η_{set} and the overall efficiency of the optical setup at the receiver η_{opt}. The field stop loss η_{FS}, is set to 0.84 for the turbulence limited filtering strategy and although current optical components are more efficient than those that operate at longer wavelengths, here the same device efficiencies are assumed for all wavelengths due to the advancement of quantum cascade lasers [64] and superconducting nanowire single-photon detectors (SNSPD) [81]. So with η_{FS}, η_{opt} and η_{det} all set to constant values, the variables that determine the behaviour of the channel efficiency are the free-space spread loss η_d and atmospheric extinction loss η_{ext}. The atmospheric extinction losses are discussed above and are a summation of the losses resulting from scattering and absorption in the atmosphere. The amount of loss due to atmospheric extinction is directly related to the wavelength of the propagating beam. The wavelength is arguably the most important parameter in the whole QKD system and is thus the focus of this research. However, it is important to investigate all of the other variables and how they relate to the wavelength.

In contrast to atmospheric extinction, the free-space spread loss is governed by the principles of diffraction and the geometric coupling efficiency can be determined using equation 3.3 which is rewritten here for convenience.

$$\eta_d = 1 - \exp\left(-\frac{1}{2}\frac{D_r^2}{w^2(\lambda, z)}\right)$$

where $w(\lambda, z)$ is given by

$$w(\lambda, z) = \sqrt{w_0^2\left[1 + \left(\frac{\lambda z}{\pi w_0^2}\right)^2\right]}$$

This diffraction-induced beam spread is responsible for a large portion of the overall loss in the channel so maximising the geometric coupling efficiency is important for realising high secret key rates. These equations allow us to identify the fundamental variables which determine the channel efficiency and ultimately the secret key rate. Once again wavelength plays an important role, further supporting the necessity of wavelength selection for QKD. The initial beam waist w_0, the propagation distance z, and the receiver diameter D_r, also play a significant role in determining the free-space loss. The geometric coupling efficiency is determined by a combination of the wavelength λ, the propagation distance z, the receiver diameter D_r and the initial beam waist w_0. Increasing either the initial beam waist or the receiver diameter will increase the geometric coupling efficiency. In contrast, increasing the wavelength or the propagation distance will decrease the geometric coupling efficiency. So as the wavelength is varied, the initial beam waist and receiver diameter must also be varied to keep the coupling efficiency constant. This suggests that larger components can make up for longer wavelengths in terms of geometric coupling efficiency but the channel efficiency is a combination of geometric and atmospheric transmission, which also varies with wavelength.

The channel efficiency determines the signal gain and ultimately the secret key rate and should be maximised if possible. However, the background probability is equally as important, especially in daylight operations. The background probability was defined in chapter 4.1 and is rewritten here for convenience.

$$Y_0 = N_b\, \eta_{det}\, \eta_{opt} + 4 f_{dark}\, \Delta t \tag{4.1}$$

The background probability is the probability of a noise photon entering the detector and it is a combination of N_b, the number of noise photons entering the field stop given by equation 3.25, and the detector dark count rate. Equation 3.25 is also rewritten here as a convenient reference point throughout this chapter.

$$N_b = \frac{H_b \Omega_{FOV} \pi D_r^2 \lambda \Delta\lambda \Delta t}{4hc} \tag{4.2}$$

The number of photons entering the field stop, and hence the background probability, is proportional to the wavelength, the receiver aperture diameter squared, the spectral and temporal filter sizes and the field stop field of view. It is important to note the quadratic relationship between receiver diameter and the number of noise photons. Although increasing the receiver size increases the channel efficiency, it also increases the number of noise photons entering the detector. This places upper limitations on secret key rate generation for each wavelength which is determined by the atmospheric transmission and spectral radiance at that wavelength. So even though some of the longer wavelengths have a reduction in solar radiation, the additional diffraction-induced beam spread requires an increase in receiver size while the longer wavelength dictates a larger field of view, see equation 3.24. Each of these in turn increases the number of noise photons able to enter the detector, so even with the reduction in spectral radiance, longer wavelengths can still let more noise photons into the detector.

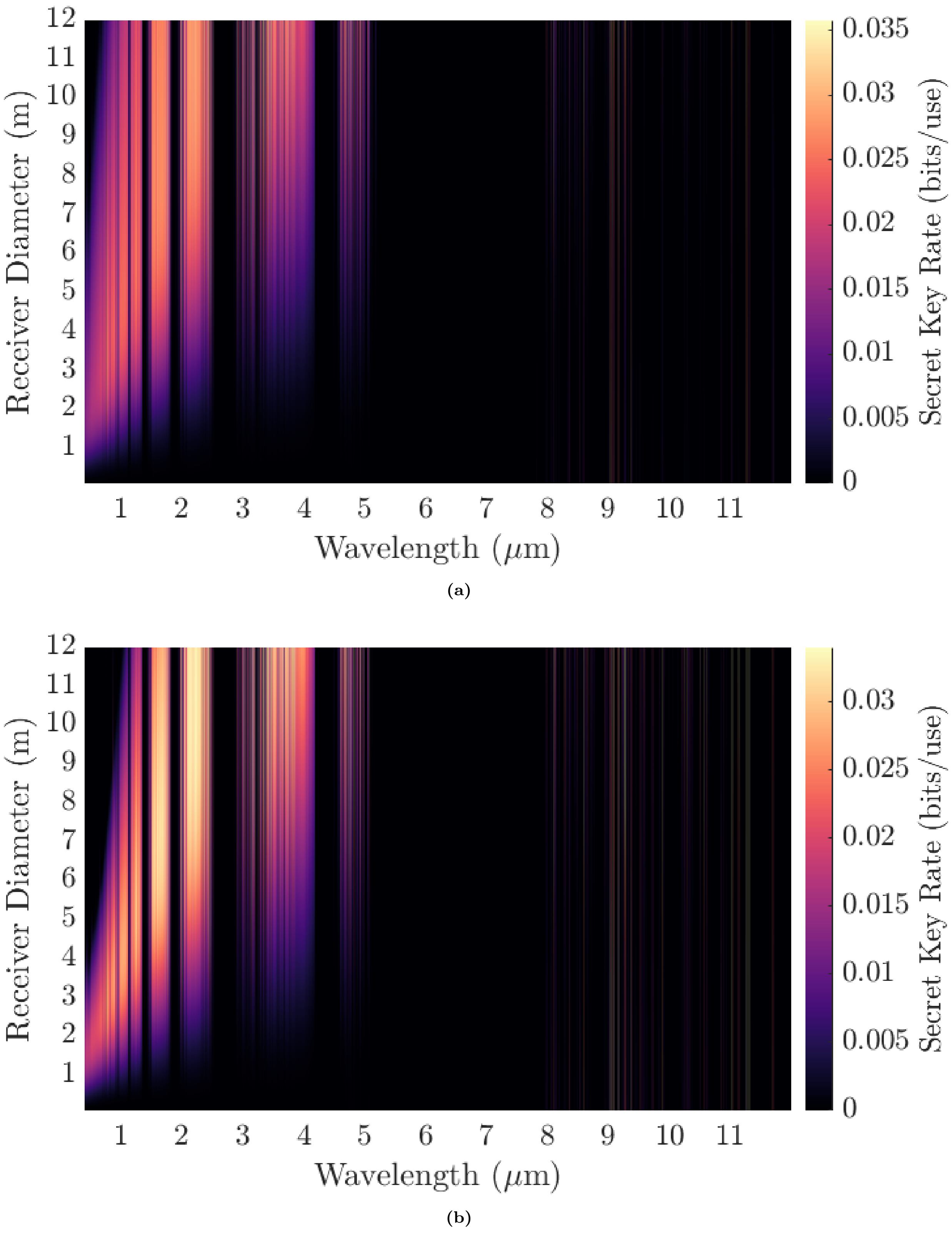
It is clear that it is important not to just consider wavelength as an isolated variable, but instead as a parameter which is intrinsically linked with other variables. As such there is no "best wavelength" for all scenarios, instead the best wavelength to use will be application-specific and depend on the conditions of that particular use case. In this work, instead of picking a set of conditions and comparing each wavelength, we wish to provide a set of re-

Name	Value
e_0	0.5
e_d	0.01
f_{ec}	1.22

Table 4.2: Summary of the constants used throughout this work to calculate the secret key rate. e_0 is the background error rate, e_d is polarization cross-talk error and f_{ec} is the error correction efficiency

sults which will inform other researchers of which wavelength is best suited to their needs. To fulfill this requirement we present a number of three-dimensional surface plots, which use the two most significant variables for downlink quantum satellite communications to calculate a range of secret key rate values. These two variables are the beam's centre wavelength λ and the diameter of the receiver aperture D_r. To account for varying initial beam waists, we construct two sets of surface plots, one for an initial beam waist of 10 cm and one using 35 cm.

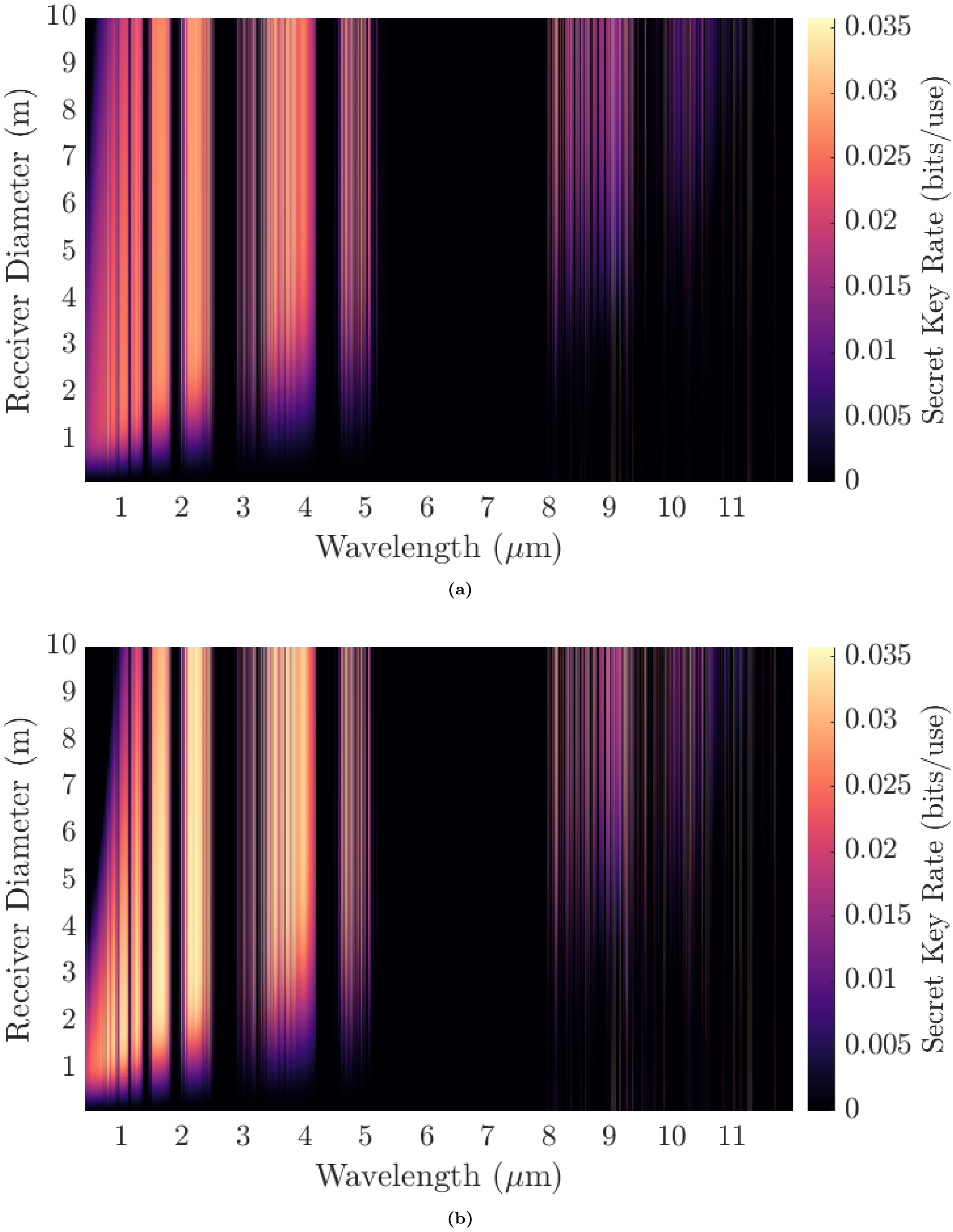
The following plots (Figure 4.5 and Figure 4.6) show surface plots with the centre wavelength on the x-axis, the receiver diameter on the y-axis and the secret key rate on the z-axis. The number of secret bits per use is represented using a colourmap, where pink corresponds to a peak in secret key rate and black corresponds to 0 or negative secret bits per use, as indicated by the colourbar. The decoy-state BB84 secret key rate is calculated using equation 3.21 for a ground receiver located at a) Waterford and b) Tucson, from a 500 km altitude satellite pointed at zenith, where the initial beam waist is alternated between 10 cm and 35 cm, the coherence length r_0 is 50 cm to represent the corrected wavefront resulting from 200 Hz adaptive optics unit. The mean photon number (MPN) of the signal-state is 0.7 while the mean photon number for the decoy-state is 0.1. Q is 1/2 for the BB84 protocol and f_{ec} is the error correction efficiency set as 1.22. The detector background count f_{dark} is 10 Hz, the background error rate e_0 is 0.5 for randomly occurring dark and background counts and the polarization cross-talk error e_d is 0.01. These parameters are summarised in tables 4.1 and 4.2.



(a)

(b)

Figure 4.5: 3D surface plot representing the secret key rate in a) Waterford and b) Tucson, for a range of receiver diameters and wavelengths when the initial beam waist is 10 cm and all other parameters are listed in tables 4.1 and 4.2



(a)

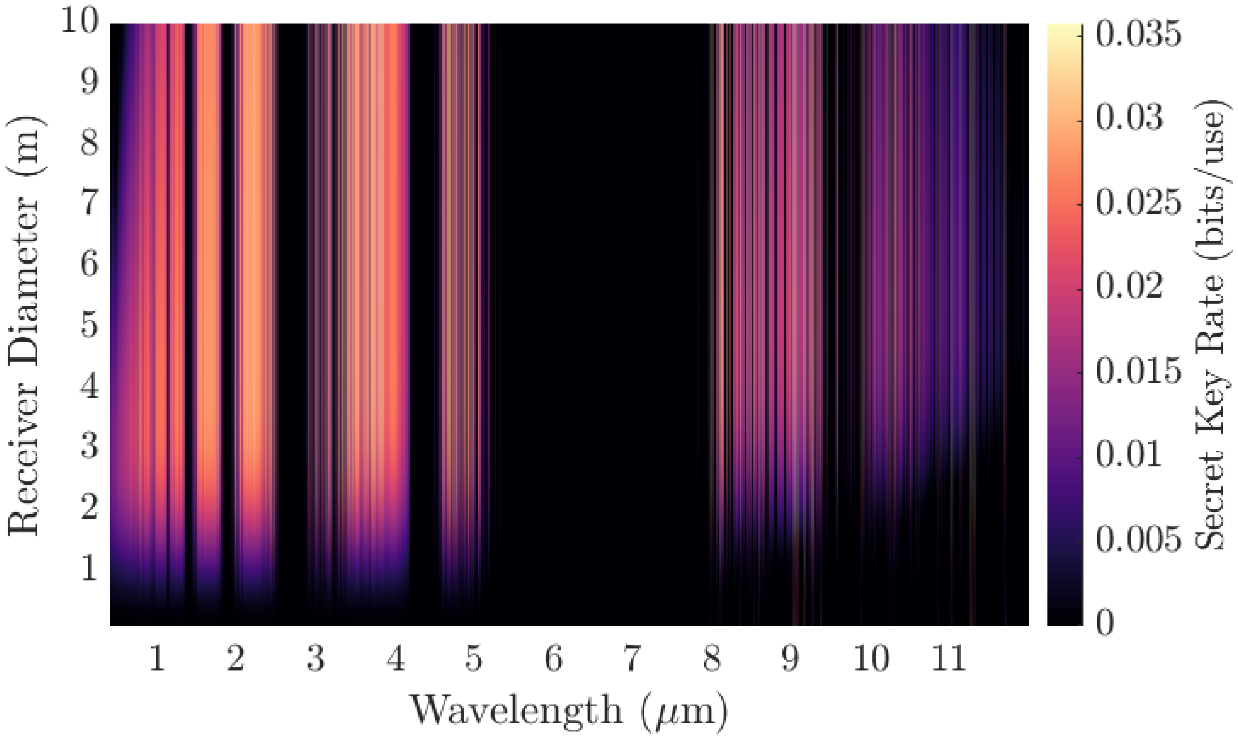
(b)

Figure 4.6: 3D surface plot representing the secret key rate in a) Waterford and b) Tucson, for a range of receiver diameters and wavelengths when the initial beam waist is 35 cm and all other parameters are listed in tables 4.1 and 4.2

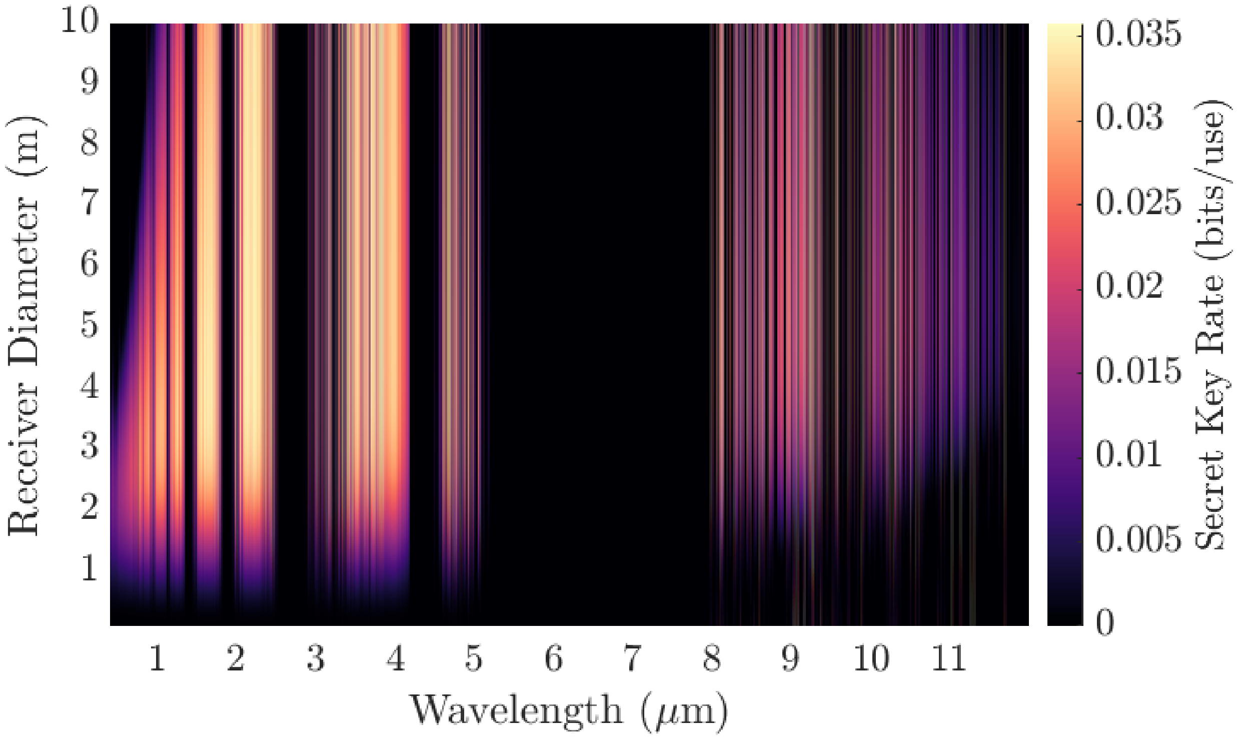
.

Figures 4.5 and 4.6 can be used to directly compare different wavelength regions and receiver size combinations. They can be used to inform researchers who wish to choose the best components for a given wavelength while also serving as a good reference for practical implementation, where the best wavelength can be selected for the component size limitations imposed by each individual use case. The wavelengths used in this plot range from 400 nm to 12 μm, providing a great visual comparison of each of the transition windows. It is interesting to compare these figures with figure 4.1 to see if the same transmission windows translate to secret key rate. While all wavelength regions that have high secret key rates do in fact have high transmission and low radiance, not all high transmission, low radiance windows correspond to high secret key rates. This is indicative of the other parameters which contribute to the secret key rate.

At a glance, these plots help identify which regions are suitable for QKD. The visible region (0.4 - 0.75 μm) performs well when the receiver size is small and the high solar radiance can be filtered out. Due to the smaller beam size at the receiver, the visible region is capable of the most stringent spatial filtering and can overcome its limitation as the window which experiences the highest level of solar radiation. The NIR (0.75 - 1.4 μm) windows have higher transmission and lower radiance than the visible window, while still benefiting from being a smaller wavelength relative to the SWIR, MWIR and LWIR. While the smaller-wavelength end of the NIR region is often used, these plots reveal that the longer wavelengths in the NIR yield the highest secret key rate across the region. The SWIR has the highest transmission across the whole spectrum while also having some of the lowest radiance. Despite being less favoured by the laws of diffraction than the visible and NIR, the SWIR has great performance across a wide range of wavelengths. There are plenty of wavelengths to use around the telecommunication wavelength at 1.55 μm, and even more beyond 2 μm. However, the SWIR requires larger receivers to achieve this superiority, especially when the initial beam waist is small. Some of the MWIR has transmission comparable to the SWIR while having even lower radiance. The region from 3 - 4 μm is usable for QKD but requires large receivers to yield similar performance to the SWIR. If the 35 cm initial beam waist is combined with large receivers, then there are pockets in the MWIR region that are capable of achieving secret key rates as high as best SWIR wavelengths. Although the LWIR has low radiance across the entire region, it suffers severely from losses due to the size of the beam waist at the receiver. Usable secret key rates are achievable if larger transmitters and receivers are used but there doesn't seem to be any benefit to using the LWIR when atmospheric conditions are good. Later we will investigate if the benefits of the LWIR in adverse weather conditions are enough to permit higher secret key rates than the lower wavelengths. The effect of changing the transmitter size can be understood by observing the differences between the plots with initial beam waist of 10 cm (Figure 4.5) and initial beam waist of 35 cm (Figure 4.6). The rate at which the beam spreads is inversely proportional to the size of the initial beam waist w_0. As we have discussed, a larger beam waist at the receiver $w(z)$ will correspond to a reduced channel efficiency due to limitations in receiver size D_r. Thus increasing the initial beam waist can affect the secret key rate in



(a)

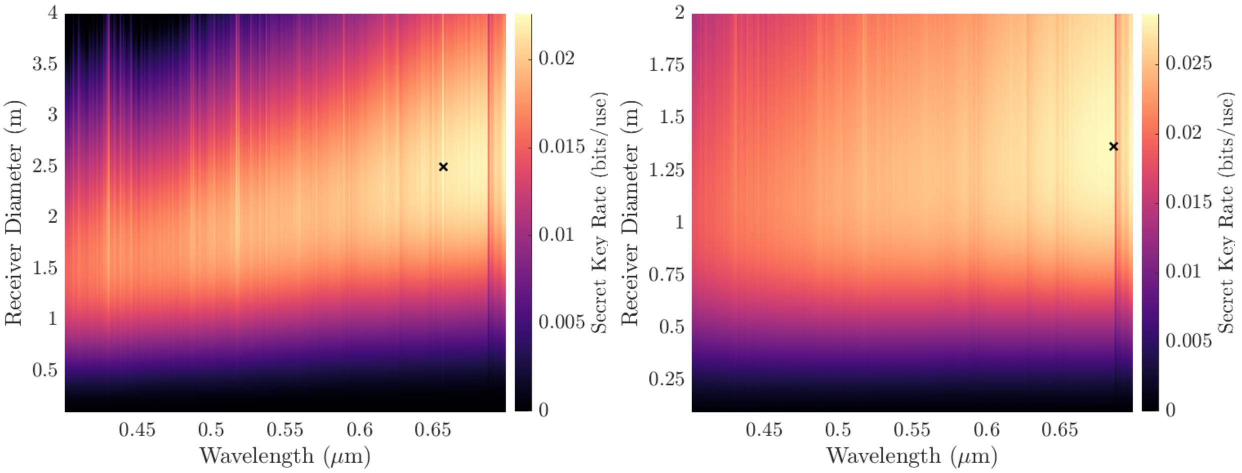


(b)

Figure 4.7: 3D surface plot representing the secret key rate in a) Waterford and b) Tucson, for a range of receiver diameters and wavelengths when the initial beam waist is 120 cm and all other parameters are listed in tables 4.1 and 4.2

two significant ways. Firstly, increasing the size of w_0 reduces the size of the beam at the receiver which means more signal reaches the detector due to the higher channel efficiency, η. This serves to increase the channel's secret key capacity, as described by the PLOB bound[41], defined as $-log2(1-\eta)$. Secondly, the reduced beam waist at the receiver that results from a larger initial beam waist, permits a reduction of the receiver aperture D_r without losing any efficiency from the channel. This is perhaps more important because a reduction in receiver aperture also corresponds to a reduction in background noise N_b, which in turn yields a higher secret key rate, R. The impact that choosing an initial beam waist has on wavelength selection is most pronounced for the longer wavelengths. In figure 4.5 when the initial beam waist is 10 cm, lower wavelengths outperform the longer wavelengths regardless of receiver size. Even when larger receivers are used to compensate for larger beam sizes associated with longer wavelengths, the LWIR struggles to generate a usable secret key rate. When the initial beam waist is increased to 35 cm, there is a huge boost in secret key rate for all wavelengths but especially for the MWIR and LWIR wavelengths. The larger initial beam waist increases the range of suitable wavelengths for QKD while reducing the receiver size and increasing the secret key rate. This phenomenon will be investigated in greater detail later in this chapter, but for now, we show the effect of increasing w0 to 1.2 m. This is shown in Figure 4.7, notice once again that MWIR and LWIR benefit from the larger initial beam waist, which has opened up much of the LWIR spectrum. However, consider that for small aperture sizes, the performance of some smaller wavelengths in the visible, NIR and SWIR regions is degraded when the initial beam waist is increased to 1.2 m. This highlights the fact that the initial beam waist is an important parameter to optimise. Fortunately, varying the w_0 within a reasonable range has little effect on which wavelengths are good for QKD and more to do with the magnitude of secret bits per use achievable for a given receiver size. Thus we can use 10 cm and 35 cm to help identify the best wavelengths from each region and afterwards, optimise both D_r and w_0 together.

Similarly, while the magnitude of the secret key and the size of the receivers are different for Waterford and Tucson, the best wavelength channels are largely the same. So for the remainder of this section, we can focus on one data set to help identify the most ideal wavelengths. We choose Tucson, as it corresponds to an ideal atmospheric and geographic location for satellite communications, achieving about 40% higher peak in secret key rate compared to the peak in Waterford. This is an interesting observation in contrast to the SNR plots from Figures 4.3 and 4.4 which indicate that Waterford has higher SNR. Later in this section, the relationship between signal to noise ratio and secret key rate is discussed in detail. Meanwhile, a finer resolution is used in MODTRAN to scan across each individual region of the electromagnetic spectrum from Visible at 400 nm to 12 μm in the LWIR. In the following plots, we use an x to mark the wavelength-receiver combination that achieves the highest secret key rate in each region. In the case of the NIR and SWIR, we show both the best wavelength across each region but also use a circle to indicate the best wavelength-receiver pair across the regions typically used for QKD due to the abundance of components. We can then quantify the difference in secret key rate and receiver size to determine if it is worthwhile to build out infrastructure for some of the less commonly used wavelengths.



(a) **(b)**

Figure 4.8: 3D surface plot representing the secret key rate across the visible region in Tucson for a range of receiver diameters when the initial beam is a) 10 cm and b) 35 cm.

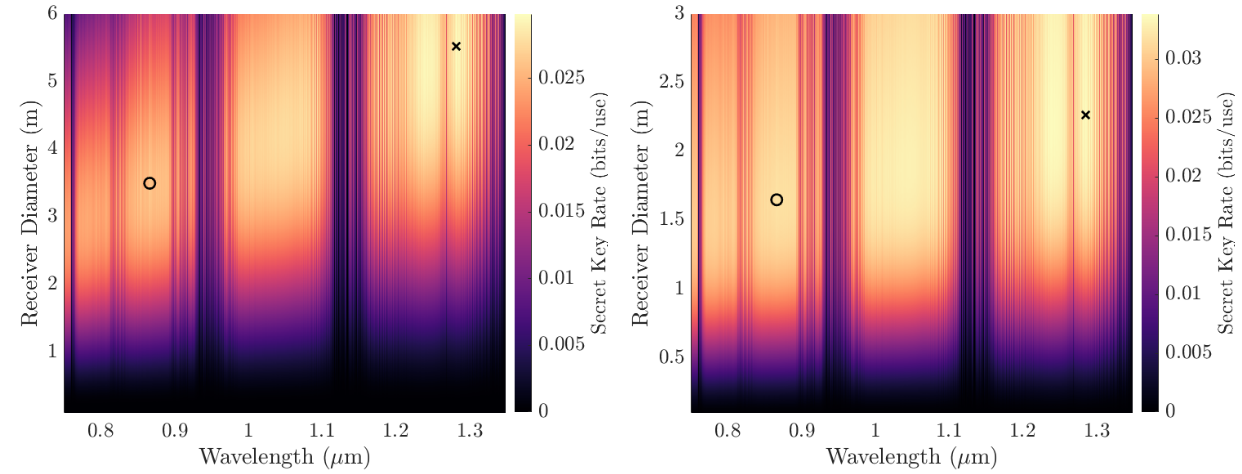


Figure 4.9: 3D surface plot representing the secret key rate across the near-infrared (NIR) region in Tucson for a range of receiver diameters when the initial beam is a) 10 cm and b) 35 cm.

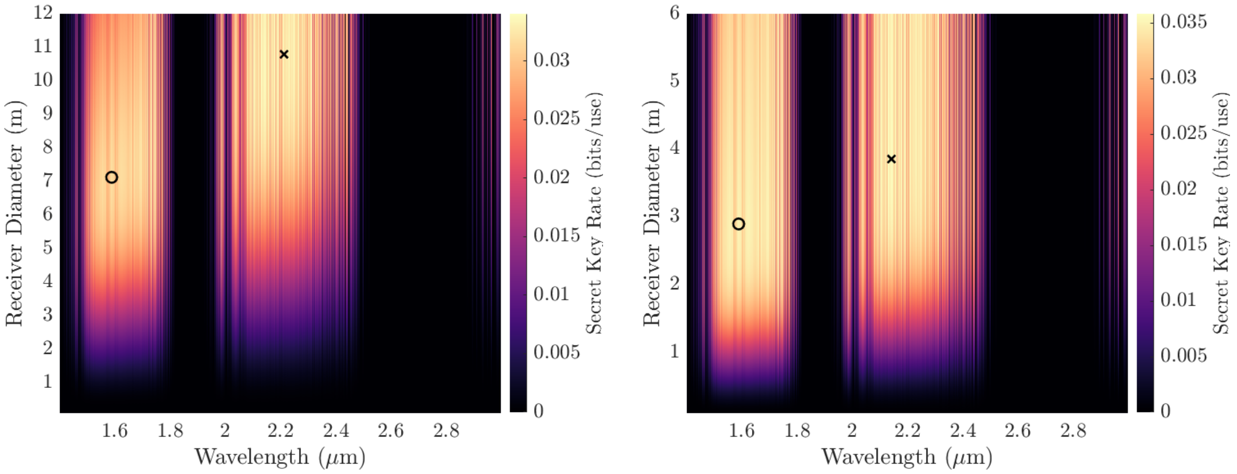


Figure 4.10: 3D surface plot representing the secret key rate across the short-wave infrared (SWIR) region in Tucson for a range of receiver diameters when the initial beam is a) 10 cm and b) 35 cm.

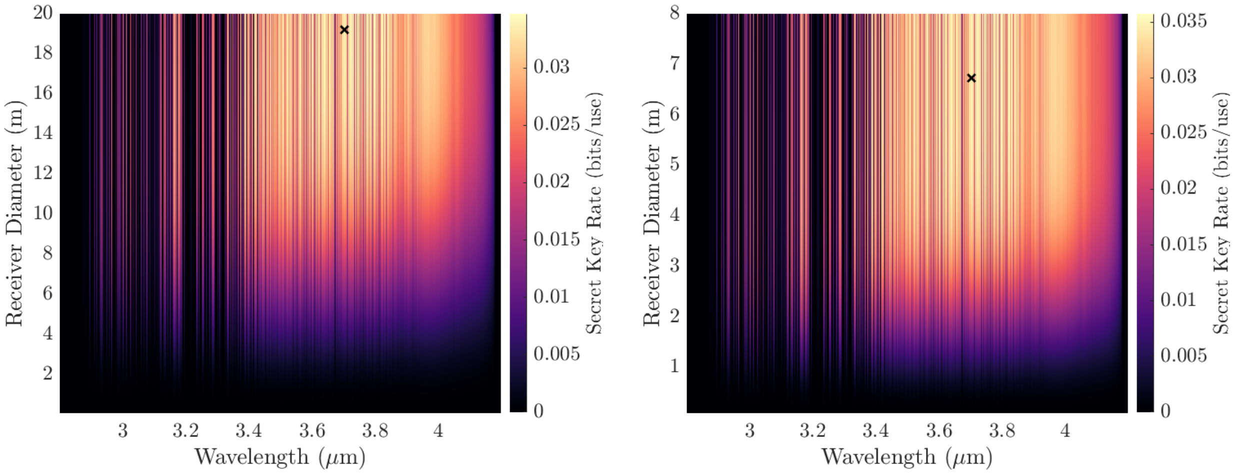


Figure 4.11: 3D surface plot representing the secret key rate across the mid-wave infrared (MWIR) region in Tucson for a range of receiver diameters when the initial beam is a) 10 cm and b) 35 cm.

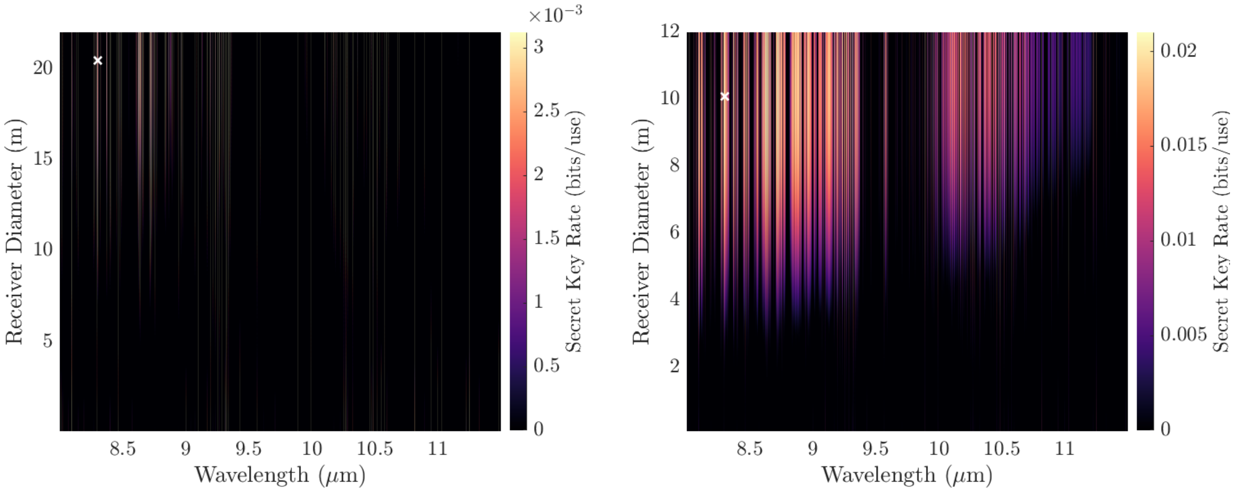


Figure 4.12: 3D surface plot representing the secret key rate across the long-wave infrared (LWIR) region in Tucson for a range of receiver diameters when the initial beam is a) 10 cm and b) 35 cm.

While Figures 4.5 to 4.7 compare each wavelength region using the same colour scale, Figures 4.8 to 4.12 each have their own colour scale. This is useful for identifying which wavelengths are the best in their region. In Figure 4.8, the visible region is plotted from 400 nm to 700 nm. Although the visible region extends to 750 nm, we have opted to exclude 700 - 750 nm. This decision was made because our algorithm found that 750 nm had the highest secret key rate but that it was too close to the typically used 780 nm wavelength in the NIR. These plots help to show how sensitive the secret key rate is to changes in wavelength and component size. These plots are more accurate than those containing the full spectrum and are used to find the optimum wavelengths and receiver sizes. We find that when the initial beam waist is 10 cm, a max secret key rate of 0.0227 bits/use is achieved with the optimum wavelength being 656.52 nm with a receiver size of 2.5 m. When the initial beam waist is increased, the secret key rate increases to 0.0287 bits/use using a receiver size of 1.39 m. It is important to note that these optimum wavelengths and receiver sizes are selected to produce the highest theoretical secret key rate. As many practical applications of QKD will require the use of smaller components, it is worthwhile to point out that when the receiver size is limited to 1 m, the best wavelength in the visible region is 430.8 nm, yielding a secret key rate of 0.0138 bits/use for a 10 w_0 cm in Tucson. This supports recent findings presented in [52] where the authors found a dip in spectral radiance near 431 nm which could provide a high secret key rate when smaller components are used.

The achievable secret key rates for the NIR spectrum are presented in Figure 4.9. Comparing the colourbar values for the NIR against the visible reveals the potential of NIR wavelengths for high-performance QKD. A number of high-performance windows emerge, including near two of the most commonly used channels, 780 nm and 850 nm. Both of these channels exist in a high transmission low radiance band, making them ideal candidates for classical and quantum satellite communications. Additionally, there is an abundance of optical components that operate at these wavelengths due to their use in the semiconductor laser industry. This combination has meant that these wavelength bands were the traditional choice for quantum key distribution. However, larger receivers permit the use of longer wavelengths to achieve higher secret key rates. A black circle is used to mark the highest secret key over the region of commonly used wavelengths for both initial beam waists. When w_0 is 10 cm, the secret key rate is 0.0275 bits/use for a wavelength of 0.8655 μm and receiver of 3.53 m but the wavelength-receiver combination that produces the highest secret key rate, 0.0297 bits/use, is a wavelength of 1.2820 μm and receiver of 5.52, which is marked as an x in Figure 4.9. When the initial beam waist w_0, is increased to 35 cm, then a secret key rate of 0.0322 bits/use is achievable using the commonly used channel centred at 0.8655 μm and a 1.69 m receiver aperture diameter while a slightly higher secret key (0.0339 bits/use) is possible if a 2.25 m receiver is combined with the channel at 1.2876 μm. While increasing the wavelength from 0.8655 μm to 1.2876 μm yields a 5 % higher secret key rate, the receiver must by increased by 33 %, so in practice, it makes a lot of sense to use 0.8655 μm channel.

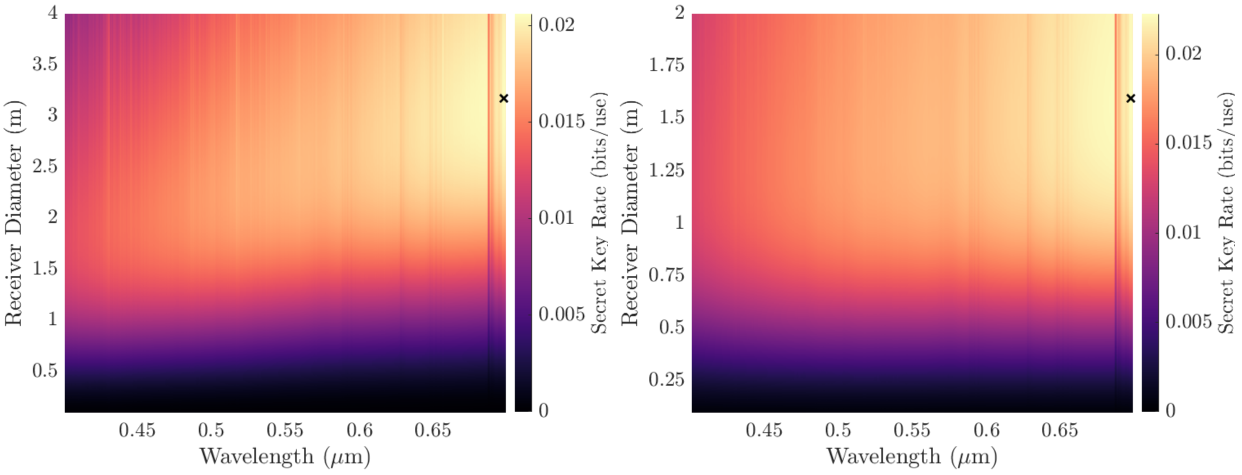
The SWIR has gained a lot of attention in recent years due to its windows of high transmission and low radiance. As the industry attempts to move beyond nighttime experiments and into daylight operations, the importance of low radiance continues to grow. However, as the wavelength increases, so to must the receiver size grow to accommodate the additional beam spread due to diffraction which in turn increases the amount of background light that gets into the detector. The SWIR region serves as a middle ground between the visible and NIR regions, to the MWIR and LWIR regions. Compared to visible and NIR wavelengths, SWIR wavelengths experience far less solar radiation and are much less susceptible to the effects of turbulence. While in comparison to the MWIR and LWIR, the effects of diffraction are much less severe, resulting in a significantly smaller beam waist at the receiver and a higher channel efficiency. These effects combine to produce the highest secret key rates across the whole electromagnetic spectrum. The channel at 1.55 μm has seen widespread use in theoretical discussions of quantum key distribution for satellite and terrestrial systems alike. This is largely due to high secret key rates and plentiful supply of devices taken from the classical telecommunications infrastructure.

However, there may be some even better wavelengths in the SWIR windows in terms of secret key rate generation. The best secret key rate emerging from the commonly used SWIR telecommunications band, for a 10 cm initial beam waist, is 0.032 bits/use which occurs at 1.5888 μm using a receiver of 7.19 m. The 1.5888 μm wavelength remains the best across this commonly used telecommunication band even when the initial beam waist is increased to 35 cm, producing a secret key rate of 0.0351 bits/use with a receiver of 2.81 m. The highest secret key rate across the whole SWIR window is from the channel centred at 2.141 μm, achieving 0.034 bits/use for a 10 cm initial beam waist requiring a 10.32 m receiver. 2.1344 μm is the best wavelength for optimizing secret key rate when the initial beam waist is 35 cm, resulting in a secret key rate of 0.358 bits/use which is the highest overall secret key rate seen in this work. While using the 35 cm initial beam waist, an extra 2% can be claimed by using the longer 2.1344 μm wavelength, the receiver size must be increased by 35%. So even though 2.1344 μm achieves a higher secret key rate, it may be more practical to continue using wavelengths near 1.55 μm. Later in this work, we find which wavelengths produce the highest secret key rate at each receiver size to quantify how worthwhile it is to increase the size of the receiver aperture in quantum key distribution systems.

The MWIR is of particular interest to this research. There is a huge dip in spectral radiance ranging from 3 - 4 μm, which corresponds with high transmission. While the extinction losses in the MWIR region are similar to those in the NIR and SWIR regions, the spectral radiance is significantly lower. This section of the MWIR region is far enough away from the peak in radiation emitted by the sun, while also being far from the peak in radiation emitted by the earth. This means that the MWIR has a significant advantage in signal to noise ratio during daylight operations as shown in Figures 4.3 and 4.4. Interestingly, this doesn't exactly translate into a big advantage in secret key rate. The performance of the MWIR for QKD is demonstrated by Figure 4.11, showing that the highest secret key rates are superior to all other regions bar the

SWIR. However, this comes at the cost of even larger receivers. To understand why the signal to noise ratio can be so much higher in the MWIR but the secret key rate is comparable to the SWIR, we must look at the equations used to calculate both values. The decoy-state BB84 signal to noise ratio is calculated by taking the signal (or decoy-state) gain and dividing it by the background probability, see equation 3.27. Note that in the decoy-state protocol the background noise is also considered part of the gain. So when the signal gain is similar, as it is for the SWIR and MWIR, then the background probability will scale the magnitude of the signal to noise ratio. This is why we see a huge difference in signal to noise between the MWIR and all other regions. In contrast, while the background probability also plays a significant role in determining the secret key rate, the number of secret bits generated per use is largely determined by the channel efficiency, see equation 3.21. As mentioned earlier, the secret key rate is limited by the PLOB bound and so even when the radiance is significantly lower, the channel cannot exceed its secret key capacity. The significant reduction in background noise in the MWIR raises the question, can novel QKD protocols be designed to exploit this advantage? In this protocol, the low background noise allows a larger receiver to be utilized without reducing the secret key rate. The highest secret key rate that can be achieved in Tucson using a MWIR wavelength of 3.7026 μm, is 0.0348 bits/use for a 10 cm initial beam waist but requires a 19.4 m receiver to obtain these highs. The receiver size can be decreased if the initial beam waist is increased, allowing a secret key rate of 0.0357 bits/use to be obtained using a 6.8 m receiver and the same 3.7026 μm wavelength.

While the LWIR has been considered for classical communications due to superior propagation through low visibility conditions, it has yet to see applications in quantum communication. Later we will see if this wavelength region can be used to generate positive key rates in unfavourable atmospheric conditions. However, in clear skies the LWIR struggles to compete with the smaller wavelengths. Although solar radiation is almost completely negligible in the LWIR, the radiation from earth peaks in this region. Additionally, the LWIR has relatively large atmospheric absorption and scattering losses. The biggest loss factor for the LWIR is due to the diffraction-induced free-space spread loss. In fact, usable secret key rates can be generated but very large transmitters and receivers are required. Perhaps the LWIR is better suited to short-range terrestrial propagation, where the reduction in attenuation through low visibility conditions and excellent propagation through turbulence can offset the additional beam spread. Although if short-ranges are used, even the beam spread can be managed. If sufficiently large components are utilized then the LWIR can achieve a secret key rate of 0.0209 bits/use using a receiver of 10.1 m, with an initial beam waist of 35 cm and a wavelength of 8.3031 μm. However, with the smaller 10 cm initial beam waist, the same wavelength only produces 0.0031 bits/use with a receiver size of 20.45 m. The results presented in this section are summarised in tables 4.3 and 4.4. Although the discussion focused on the Tucson results, the Waterford results are shown in Figures 4.13 to 4.17 and the best wavelengths and receiver sizes are shown in tables 4.5 to 4.6. The results are similar for both scenarios with both conditions following the same trend for channel selection. The centre wavelength is slightly different due to variations in transmittance and radiance but the most significant difference is the size of receivers required and the maximum secret key rates. Tucson achieves a much higher secret key rate due to lower absorption and scattering while the reduced spectral radiance in Waterford permits use of larger receivers to improve the channel efficiency.



(a) **(b)**

Figure 4.13: 3D surface plot representing the secret key rate across the visible region in Waterford for a range of receiver diameters when the initial beam is a) 10 cm and b) 35 cm.

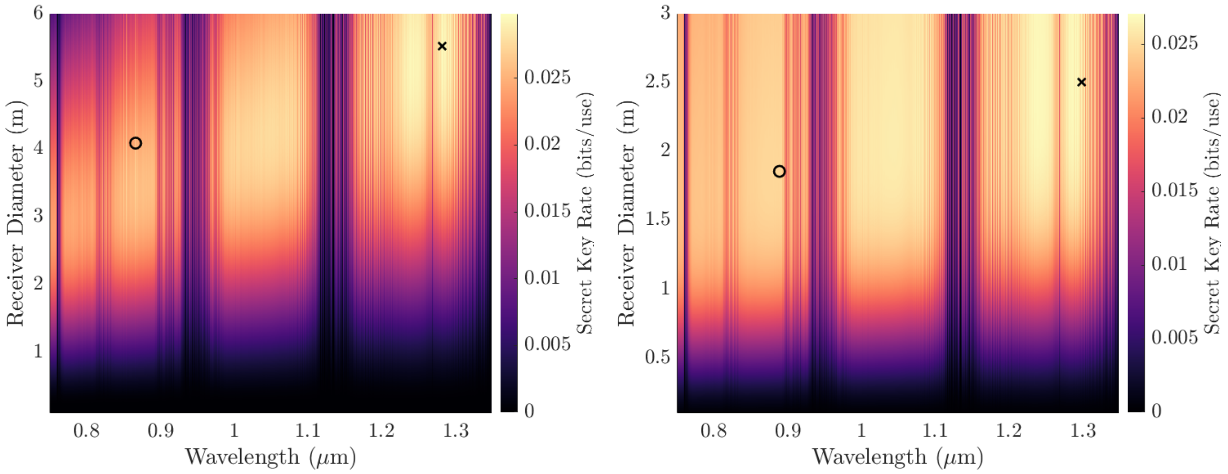


Figure 4.14: 3D surface plot representing the secret key rate across the near-infrared (NIR) region in Waterford for a range of receiver diameters when the initial beam is a) 10 cm and b) 35 cm.

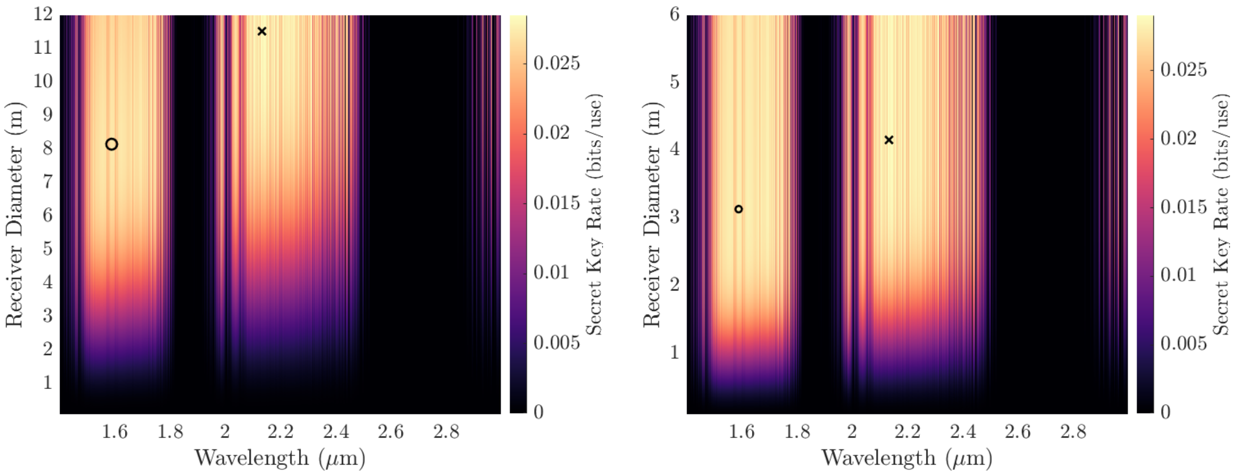


Figure 4.15: 3D surface plot representing the secret key rate across the short-wave infrared (SWIR) region in Waterford for a range of receiver diameters when the initial beam is a) 10 cm and b) 35 cm.

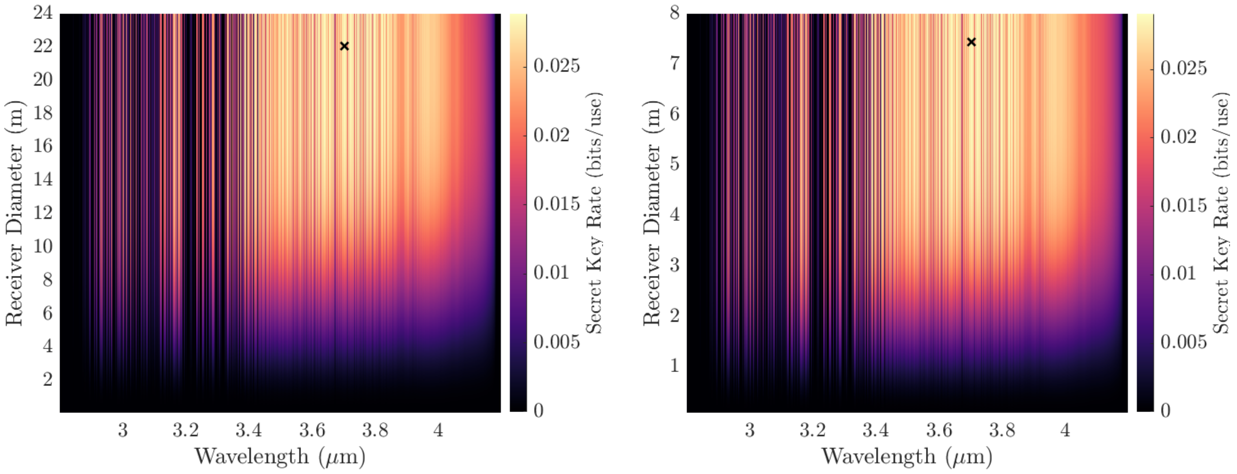


Figure 4.16: 3D surface plot representing the secret key rate across the mid-wave infrared (MWIR) region in Waterford for a range of receiver diameters when the initial beam is a) 10 cm and b) 35 cm.

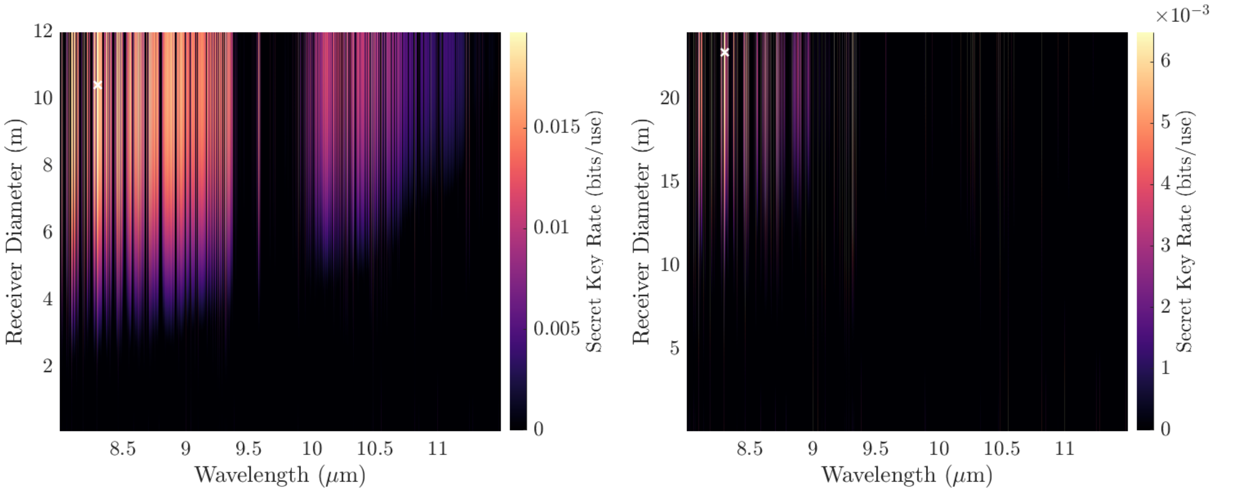


Figure 4.17: 3D surface plot representing the secret key rate across the long-wave infrared (LWIR) region in Waterford for a range of receiver diameters when the initial beam is a) 10 cm and b) 35 cm.

Visible	NIR	SWIR	MWIR	LWIR	NIR_Typical	SWIR_Typical	Type
0.65652	1.282	2.1414	3.7026	8.3031	0.86645	1.58885	λ (µm)
2.502	5.5232	10.3172	19.397	20.4515	3.5313	7.1919	D_r (m)
0.0227	0.0297	0.034	0.0348	0.0031	0.0275	0.032	SKR (bits/use)

Table 4.3: Results for the best wavelength-receiver combinations for each transmission window in Tucson when the initial beam waist is 10 cm

Visible	NIR	SWIR	MWIR	LWIR	NIR_Typical	SWIR_Typical	Type
0.69739	1.2857	2.1344	3.7026	8.3031	0.86645	1.58885	λ (µm)
1.3859	2.3051	3.7949	6.803	10.0768	1.696	2.8131	D_r (m)
0.0287	0.0339	0.0358	0.0357	0.0209	0.0322	0.0351	SKR (bits/use)

Table 4.4: Results for the best wavelength-receiver combinations for each transmission window in Tucson when the initial beam waist is 35 cm

Visible	NIR	SWIR	MWIR	LWIR	NIR_Typical	SWIR_Typical	Type
0.69739	1.2988	2.1318	3.7026	8.303	0.86654	1.5888	λ (µm)
3.1727	6.2444	11.5192	22.3101	22.7929	4.0899	8.1535	D_r (m)
0.0206	0.0256	0.0284	0.0289	0.0065	0.0235	0.0273	SKR (bits/use)

Table 4.5: Results for the best wavelength-receiver combinations for each transmission window in Waterford when the initial beam waist is 10 cm

Visible	NIR	SWIR	MWIR	LWIR	NIR_Typical	SWIR_Typical	Type
0.69739	1.2988	2.1407	3.7026	8.303	0.88905	1.5888	λ (µm)
1.597	2.4939	4.1697	7.5	10.4808	1.85556	3.1323	D_r (m)
0.0223	0.0271	0.029	0.0291	0.0197	0.0249	0.0282	SKR (bits/use)

Table 4.6: Results for the best wavelength-receiver combinations for each transmission window in Waterford when the initial beam waist is 35 cm

4.3 Practical Quantum Key Distribution

In this chapter, the secret key rate was optimised in Waterford and Tucson by varying the wavelength, initial beam waist and receiver diameter. This allowed a direct comparison of each of the wavelength regions, and while it is useful for a theoretical discussion of what is possible, it serves as a best-case scenario for each region. In the following section, practical size limitations and realistic atmospheric conditions are considered to determine what wavelengths are suitable for real-world satellite quantum communications.

4.3.1 Optimizing Components Sizes for Secret Key Rate

In this section, the wavelengths that have demonstrated the highest secret key rates in the previous section, are analysed and compared. One wavelength is selected to represent its corresponding transmission window and in the following sections, the performance of each wavelength is compared in a range of turbulent strengths. In this section, the optimum component sizes for maximising secret key rate are selected for each wavelength. In the earlier sections, only two initial beam waists are used, 10 cm and 35 cm. Now, the initial beam waist is varied between 0.1 and 1.2 m to find the ideal component sizes for each wavelength. As has already been discussed, when attempting to maximise the secret key rate, the initial beam waist is intrinsically tied to the receiver diameter so they should be optimised together. In Figure 4.18, a set of 3D contour plots are shown, representing the secret key rate in Tucson, for a range of receiver diameters and initial beam waists. The most ideal wavelengths for maximising secret key rate are selected from Figures 4.8 - 4.12, to represent the behaviour of each propagation window. The secret key rate is calculated using the parameters listed in tables 4.1 and 4.2.

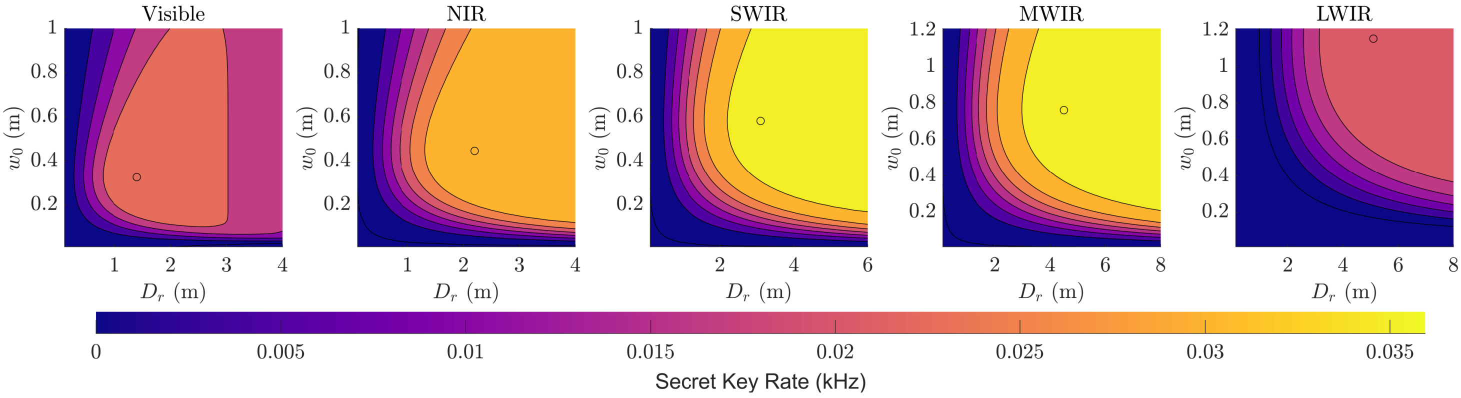


Figure 4.18: 3D contour plot representing the secret key rate in Tucson, for a range of receiver diameters and initial beam waists. The highest performing wavelength is selected to represent each propagation window and the receiver-initial beam waist pair that produces the highest secret key rate for each wavelength is indicated with black circle, as determined using the parameters listed in tables 4.1 and 4.2

The 5 contour plots all use the same colourscale, making it easy to compare the performance of each of the wavelengths. These plots are designed to help find the initial beam waist and

Parameter	Visible	NIR	SWIR	MWIR	LWIR	NIR (Typical)	SWIR (Typical)
λ (μm)	0.69739	1.2857	2.1344	3.7026	8.3031	0.86645	1.58885
SKR (bits/use)	0.0287	0.0339	0.036	0.0358	0.0246	0.0322	0.0352
D_r (m)	1.3784	2.1613	3.1423	4.5	5.1342	1.6757	2.5477
w_0 (m)	0.3261	0.4465	0.5819	0.7625	1.1538	0.3712	0.5067

Table 4.7: The best wavelength, receiver diameter and initial beam waist combinations for maximising secret key rate in Tucson at each wavelength as extracted from Figure 4.18 using the parameters listed in tables 4.1 and 4.2. The optimal pair is marked with a circle in Figure 4.18.

receiver size pair that maximises secret key rate to identify which wavelength region holds the most potential for high data rates. Additionally they can be used to determine the best transmission window to use in a scenario that places size limitations on w_0 or D_r. In the case of the downlink channel, the transmitter sits on-board the satellite which places size limitations on w_0. Using these plots, for a given w_0, the best wavelength and receiver size can be identified. Similarly, if there is a size limitation for the ground receiver, these plots can be used to identify the required wavelength and w_0 to achieve a high secret key rate. Figure 4.19 shows a similar plot for optimizing the components required to generate the highest secret key rates in the Waterford scenario. Optimising the transmitting and receiving components can improve secret key rate slightly but the biggest benefit to increasing the initial beam waist is a reduction in required receiver size. For example, if w_0 is increased from 35 cm to 76.25 cm, then the receiver size required to obtain the maximum secret key rate for the MWIR wavelength, is reduced from 6.8 m to 4.5 m in Tucson and from 7.5 m to 4.94 m in Waterford. The best wavelength-receiver-initial beam waist combinations for each wavelength region and the maximum secret key rate they produce are presented in Table 4.7 for Tucson and Table 4.8 for Waterford.

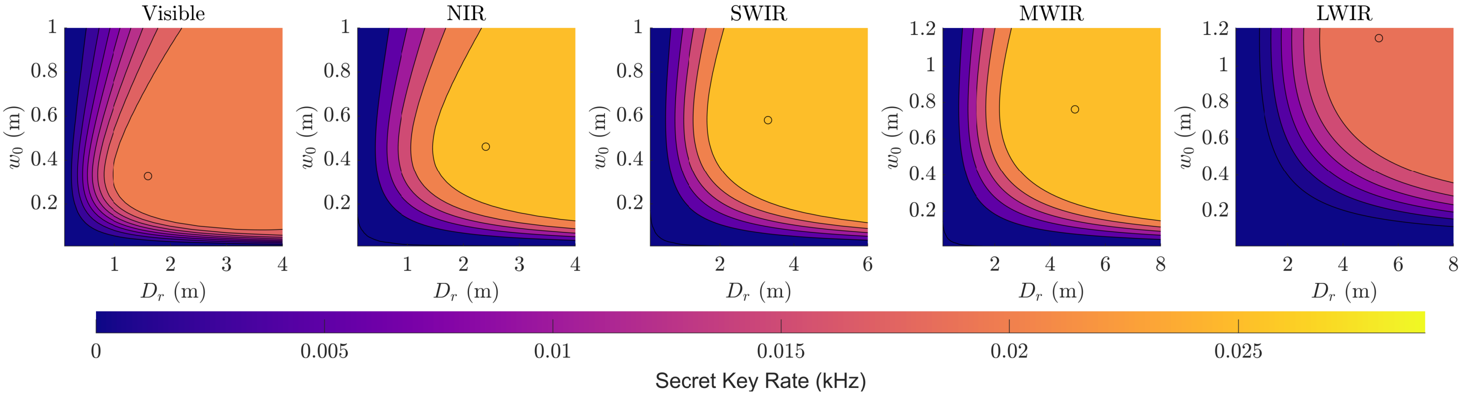


Figure 4.19: 3D contour plot representing the secret key rate in Waterford, for a range of receiver diameters and initial beam waists. The highest performing wavelength is selected to represent each propagation window and the receiver-initial beam waist pair that produces the highest secret key rate for each wavelength is indicated with black circle, as determined using the parameters listed in tables 4.1 and 4.2

.

Parameter	Visible	NIR	SWIR	MWIR	LWIR	NIR (Typical)	SWIR (Typical)
λ (μm)	0.69739	1.2988	2.1407	3.7026	8.303	0.88905	1.5888
SKR (bits/use)	0.0223	0.0271	0.029	0.0291	0.0222	0.0249	0.0282
D_r (m)	1.5865	2.3694	3.3405	4.936	5.273	1.8541	2.7856
w_0 (m)	0.3261	0.4615	0.5819	0.7625	1.1538	0.3712	0.5067

Table 4.8: The best wavelength, receiver diameter and initial beam waist combinations for maximising secret key rate in Waterford at each wavelength as extracted from Figure 4.19 using the parameters listed in tables 4.1 and 4.2. The optimal pair is marked with a circle in Figure 4.19.

4.3.2 Optimum Wavelength Selection Through Atmospheric Turbulence

Throughout this work, the 200 Hz adaptive optics system has been used to boost secret key rate and now, we investigate how such a system affects performance. In Figures 4.20 and 4.21 we plot secret key rate for a range of coherence lengths using the optimal receiver and beam sizes for each wavelength, as determined in the previous section. The vertical lines at 5 cm and 50 cm are adopted from reference [52] and are a description of the wavefront resulting from uncompensated turbulence and post adaptive optics correction, respectively. This plot is useful for characterising the impact that an adaptive optics unit has on secret key rate while also determining what wavelengths will yield the best performance through turbulence. Recall

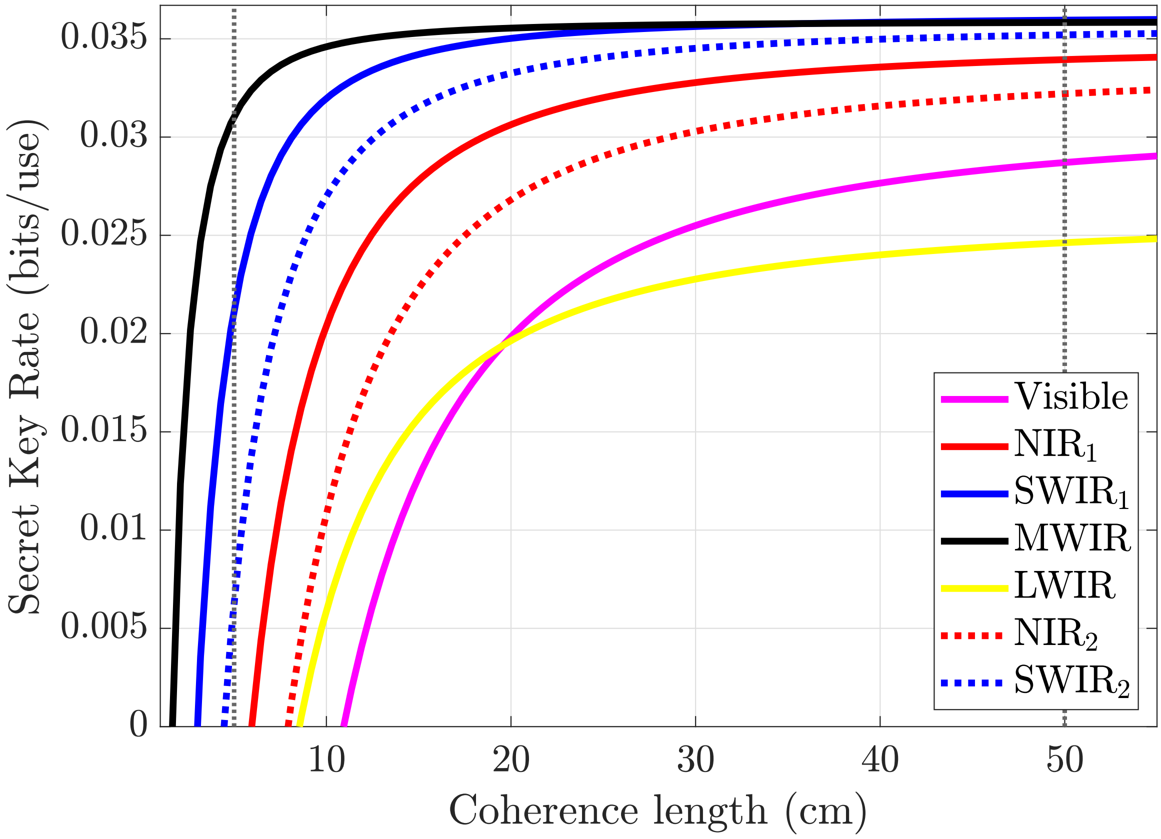


Figure 4.20: Secret key rate in Tucson is plotted a range of coherence lengths using the optimal receiver and beam sizes for each wavelength, as determined in the previous section.

that the coherence length $r_0(\lambda)$ is inversely proportional to strength of turbulence. Notice the significant increase in performance gained by using an adaptive optics unit for most most wavelengths. When the turbulence is compensated for by the 200 Hz adaptive optics system, the SWIR and MWIR yield the best performance, followed by the NIR, visible and then LWIR wavelengths. However, if the coherence length is low, indicating turbulence-induced wavefront aberrations, the MWIR stands out and performs significantly better than other wavelengths. Even when the coherence length is as low as 5 cm, representing a completely uncompensated turbulence-distorted wavefront, the MWIR performs better than the visible and LWIR do, even after they are compensated by a 200 Hz adaptive optics system. Thus the MWIR could be used as an alternative to Adaptive Optics. Additionally, turbulence-induced beam spread is the biggest loss factor in the uplink so perhaps the MWIR could overcome some of this loss and achieve usable secret key rates. This plot also compares the performance of the best NIR and SWIR wavelengths with wavelengths more typically used in these regions due to the abundance of devices. When the turbulent effects are compensated by a suitable AO system, there is not a large difference in secret key rate between the best in the NIR and SWIR and the more commonly used NIR and SWIR wavelengths. However, when the turbulence-induced wavefront distortions are uncompensated as indicated by the 5 cm coherence length, the secret key rate is much larger for the best wavelengths in each region. Therefore when operating through strong turbulence or in normal turbulence conditions without an adaptive optics system, then it may be more beneficial to use the best wavelengths in each region, which means increasing the wavelength and the component size for both the NIR and SWIR regions.

4.3.3 Receiver and Transmitter Size Limitations

So far, the wavelength regions have been compared in the context of high secret key rate generation. It became clear that a number of variables ultimately determine the ideal wavelength, these variables include the propagation distance, turbulence strength, the transmitter size and the receiver size. In the previous sections, the initial beam waist, receiver size and wavelength were optimised to determine ideal QKD generation rates. However, in real-world applications, the secret key rate must be optimised whilst abiding by component size limitations. For example, the MWIR wavelength can achieve similarly high-performance to the SWIR wavelength but requires very large transmitters and receivers, which make it impractical to realise on commercial satellites. While some of the plots shown earlier are helpful for determining the absolute highest secret key rates, Figure 4.22 shows that many of the optimum wavelengths used earlier, no longer perform well when the receiver size is limited. These figures show that the trade-off between receiver size and QKD performance is also a trade-off in optimum wavelength. Throughout most of this work, the SWIR channel at 2.134 μm and the MWIR channel at 3.703 μm have consistently yielded the highest QKD performance but when the receiver size is limited below 2 m, these wavelengths are outperformed by smaller wavelengths in the visible, NIR and shorter end of the SWIR region. In this section, the highest performing wavelengths are selected based

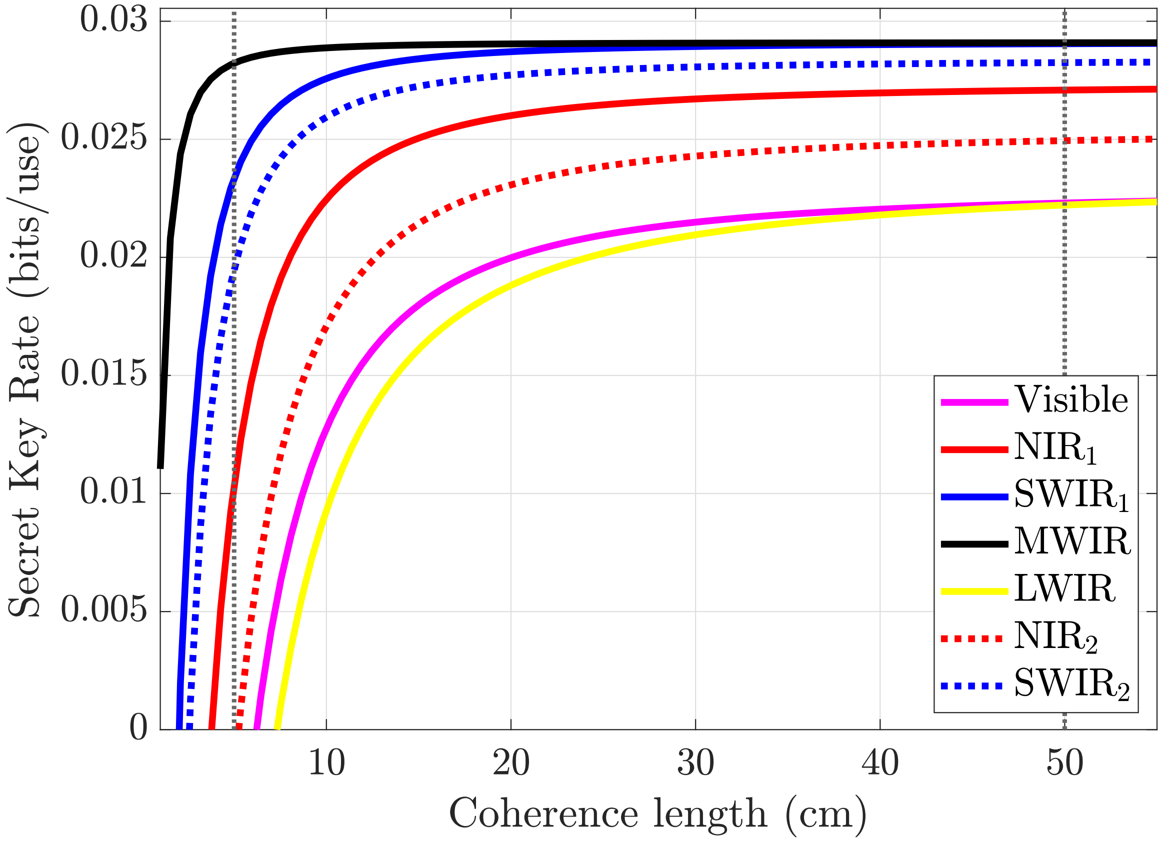
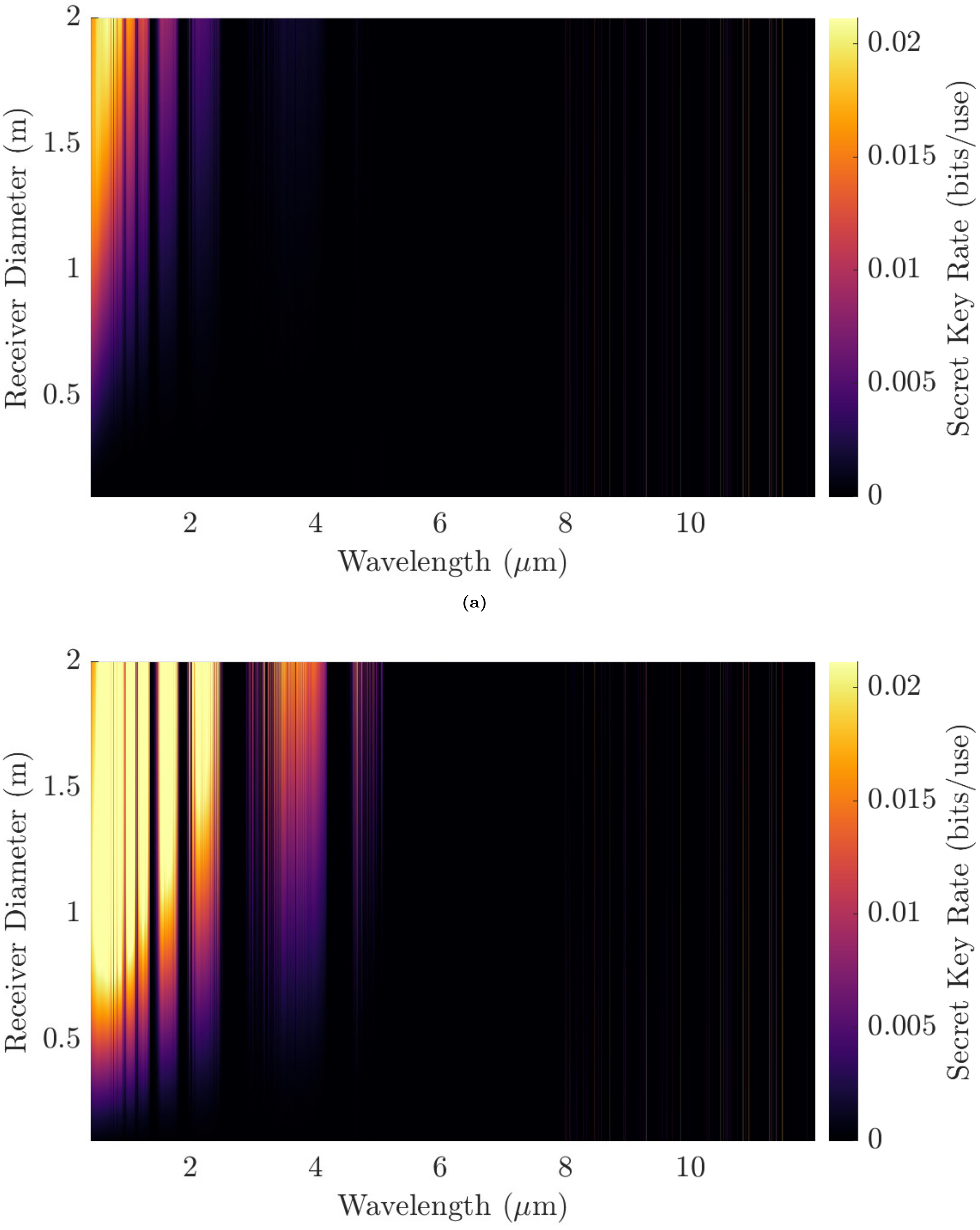


Figure 4.21: Secret key rate in Waterford is plotted a range of coherence lengths using the optimal receiver and beam sizes for each wavelength, as determined in the previous section.

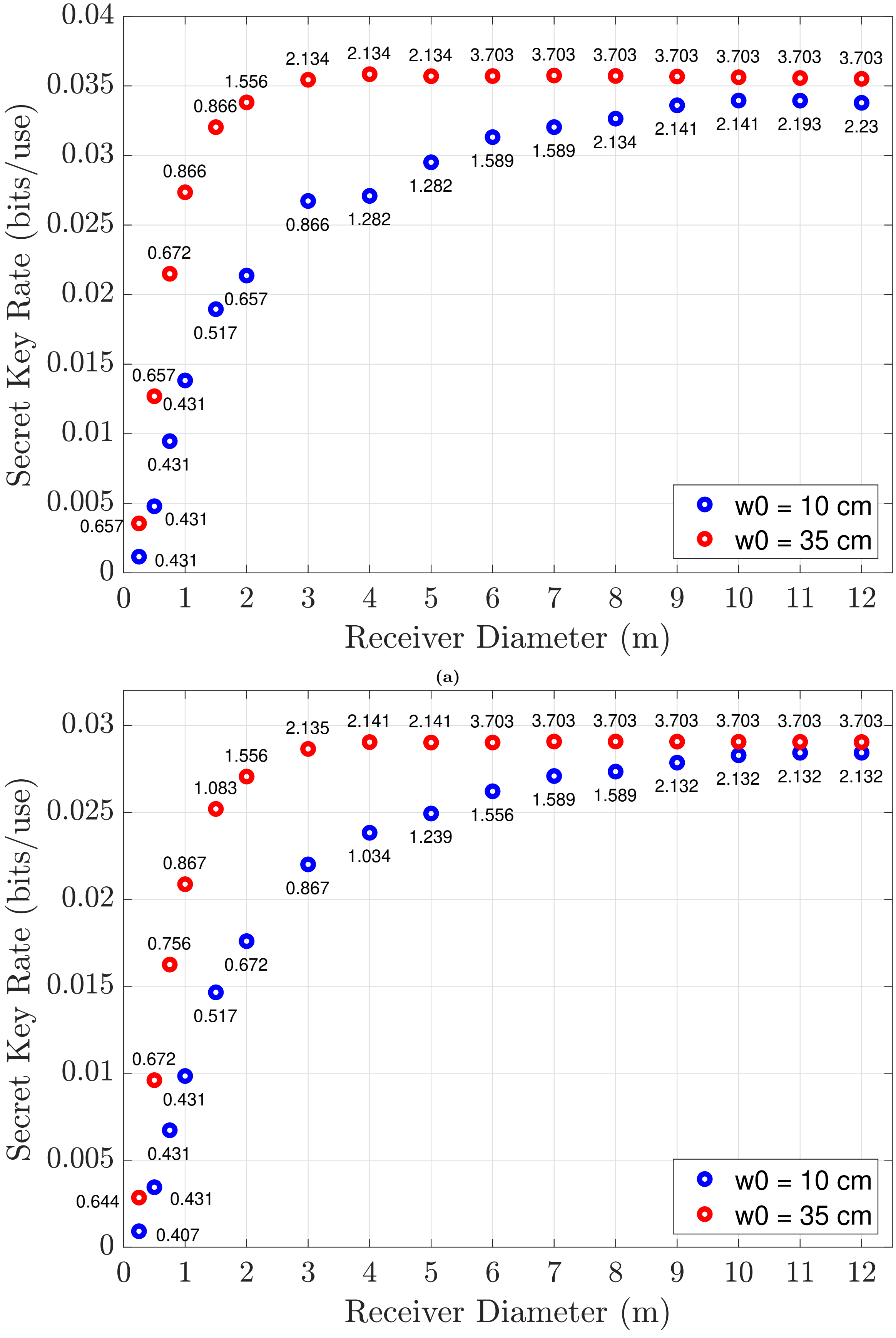
on a given set of component size limitations. In Figure 4.23, the maximum secret key rates across the entire spectrum, are plotted against receiver diameter in a) Tucson and b) Waterford. At each point on the graph, the corresponding wavelength that produces the secret key rate for each receiver diameter is shown next to the data point. Data is shown for receiver diameters of 0.25 m, 0.5 m, 0.75 m, 1 m, 1.5 m and then in 1 m increments from 2 m - 12 m. Once again, two data sets are presented to show the effect of varying the initial beam waist. The blue points correspond to an initial beam waist of 10 cm while the red data points correspond to an initial beam waist of 35 cm. The results are similar for both Tucson and Waterford so rather than discuss both, the results for Tucson are analysed while any differences in optimum wavelength are displayed in tables 4.9 and 4.10. Interestingly when the initial beam waist is 10 cm and the receiver diameter is less than or equal to 1 m, the channel at 0.431 μm produces the highest secret key rate. Over the same range, the 35 cm initial beam waist increases the secret key rate and as the receiver size increases, so does the optimum wavelength. 0.657 μm is best when the receiver diameter is less than or equal to 0.5 m but at 075 m, a slightly longer 0.672 μm channel achieves a significantly higher secret key rate. At 1 m the channel at 0.886 μm achieves a secret key rate of 0.02735 bits/use when the initial beam waist is 35 cm, almost twice as high compared to the same receiver size but using a 10 cm beam waist (0.01383 bits/use) and over 7 times higher than the secret key rate using a receiver of 0.25 m, 0.001164 bits/use and 0.003554 bits/use for the 10 cm and 35 cm initial beam waists respectively. Increasing the receiver size



(a)

(b)

Figure 4.22: 3D surface plot representing the signal to noise ratio in Tucson for a range of receiver diameters and wavelengths when the initial beam waist is a) 10 cm and b) 35 cm. All other parameters are listed in tables 4.1 and 4.2.



(a)

(b)

Figure 4.23: Showing the effect that increasing the initial beam waist and receiver diameter has on the maximum secret key rate and optimum wavelength selection in a) Tucson and b) Waterford. The labeled data points show which wavelength (μm) produces the maximum secret key rate for each initial beam waist and receiver size combination.

has profound effects on secret key rate, especially when D_r is less than 1 m. Increasing to 1.5 m increases the 10 cm initial beam waist secret key rate by 37 % to 0.01895 bits/use and the 35 cm initial beam waist secret key rate by 17% to 0.03203 bits/use. These rates are achieved using the channel at 0.517 μm for the 10 cm initial beam waist and 0.886 μm for the 35 cm initial beam waist. Increasing the receiver size larger than 1.5 m starts to have diminishing returns, as more noise photons enter the detector. Increasing to 2 m yields a 12.7 % improvement in secret key rate for 10 cm initial beam waist but only a 5.5 % for the larger initial beam waist, when the wavelength is increased to 0.657 μm and 1.556 μm for the 10 cm and 35 cm initial beam waists respectively. While the 10 cm initial beam waist system continues to benefit from increasing the receiver diameter, the secret key rate achievable with the 35 cm initial beam waist starts to saturate after 3 m, reaching a peak of 0.0358 bits/use at 3.8 m with a 2.134 μm wavelength. The MWIR channel centred at 3.703 μm is almost capable of reaching the same highs but requires a receiver size of 6 m. In contrast, the 10 cm initial beam waist condition doesn't reach its maximum (0.03395 bits/use) until a receiver size of 10 m, using a wavelength of 2.141 μm. However, for a 6 m receiver used with the same initial beam waist, the channel at 1.589 μm is capable of reaching a secret key rate of 0.03132 bits/use. So although the channel centred at 2.134 produces the highest secret key rates, large transmitters and receivers are required, meanwhile similar performance can be obtained using the channel at 1.556 μm and a 2 m aperture. Considering the abundance of optical devices optimised for this channel, it seems likely that it is the most practical channel for satellite QKD. If using a smaller initial beam waist, then larger receiver apertures are required to generate high secret key rates although usable rates can be generated using an aperture diameter as small as 0.25 m, provided a small visible wavelength is used to overcome diffraction losses associated with long-range propagation.

D_r (m)	0.25	0.5	0.75	1	1.5	2	3	4	5	6	7	8	9	10	11	12
λ (μm)	0.431	0.431	0.431	0.431	0.517	0.657	0.866	1.282	1.282	1.589	1.589	2.134	2.141	2.141	2.193	2.23
λ (μm)	0.407	0.431	0.431	0.431	0.517	0.672	0.867	1.034	1.239	1.556	1.589	1.589	2.132	2.132	2.132	2.132

Table 4.9: The best wavelengths at each receiver diameter D_r, for an initial beam waist of 10 cm in Tucson (middle row) and Waterford (bottom row).

D_r (m)	0.25	0.5	0.75	1	1.5	2	3	4	5	6	7	8	9	10	11	12
λ (μm)	0.657	0.657	0.672	0.866	0.866	1.556	2.134	2.134	2.134	3.703	3.703	3.703	3.703	3.703	3.703	3.703
λ (μm)	0.644	0.672	0.756	0.867	1.083	1.556	2.135	2.141	2.141	3.703	3.703	3.703	3.703	3.703	3.703	3.703

Table 4.10: The best wavelengths at each receiver diameter D_r, for an initial beam waist of 35 cm in Tucson (middle row) and Waterford (bottom row)

4.3.4 Adverse Weather Conditions

Up to this point, the scenarios considered have permitted relatively high QKD performance. While the data used for Tucson is quite realistic, it does not reflect most atmospheric conditions around the world. While Waterford's atmospheric conditions are more typical, we have only considered propagation through light, mostly transparent clouds. However, in reality, Waterford winter skies often experience a range of adverse weather conditions. Considering historical hourly weather reports and model reconstructions for noon on December 21st [111], there is more than a 60% chance of mostly cloudy or overcast weather and a 39% chance of rain falling throughout the day. In this section, the performance of each wavelength is compared in these unfavourable conditions.

A number of conditions were considered including radiative fog with 500 m visibility, drizzle rain clouds and haze which is defined here as light fog with a 5 km visibility. Other cloud types were considered such as stratus, stratocumuls and moderate rain but all had even greater attenuation than the drizzle rain clouds. In Figure 4.24, the transmission and radiance are plotted from 400 nm at Waterford in the presence of a 5 km visibility radiative haze. Figure 4.24 demonstrates the superior propagation of the LWIR in conditions of low visibility. In contrast to LWIR the visible, NIR, SWIR and MWIR are severely attenuated in haze. The LWIR is also attenuated by haze but significantly less than the other regions.

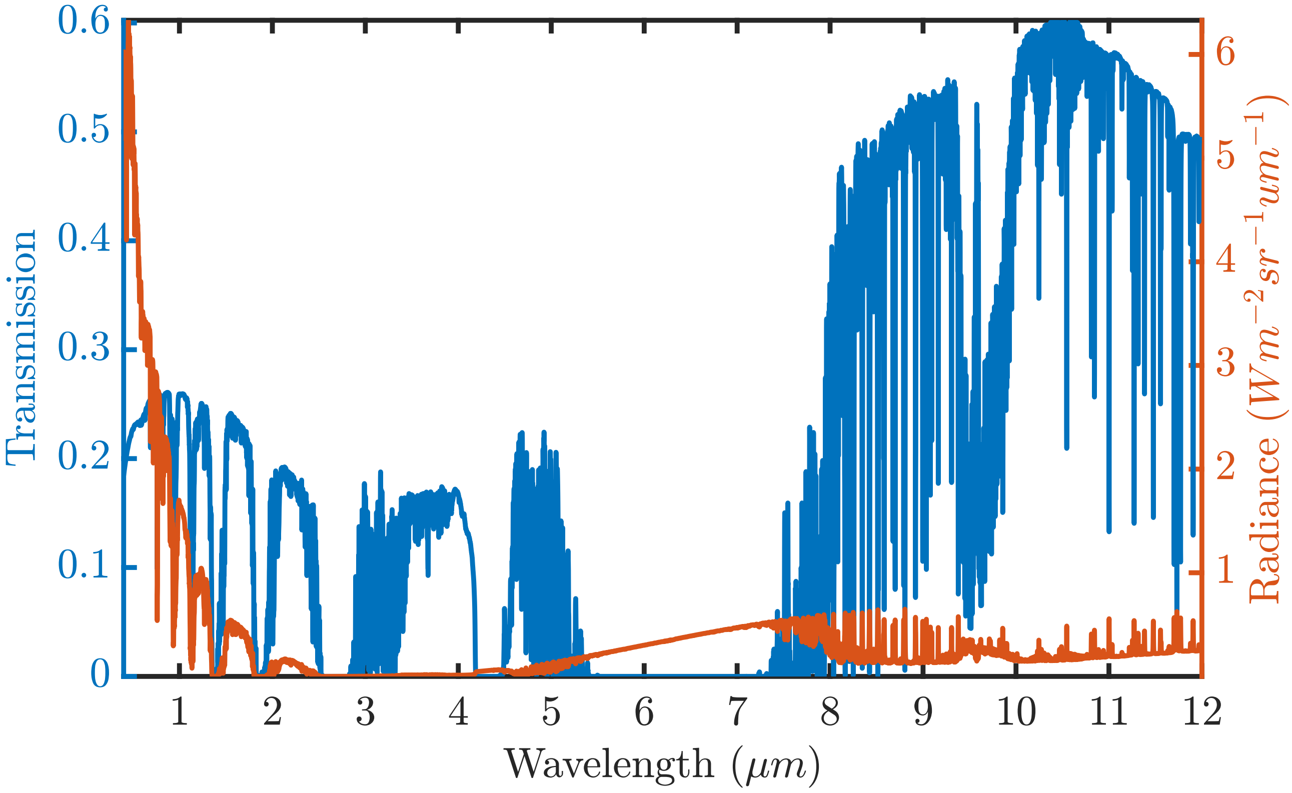


Figure 4.24: Transitivity and radiance plotted as a function of wavelength, for a ground receiver pointed at zenith at 12 pm noon on the winter solstice in Waterford, through a 5 km visibility haze.

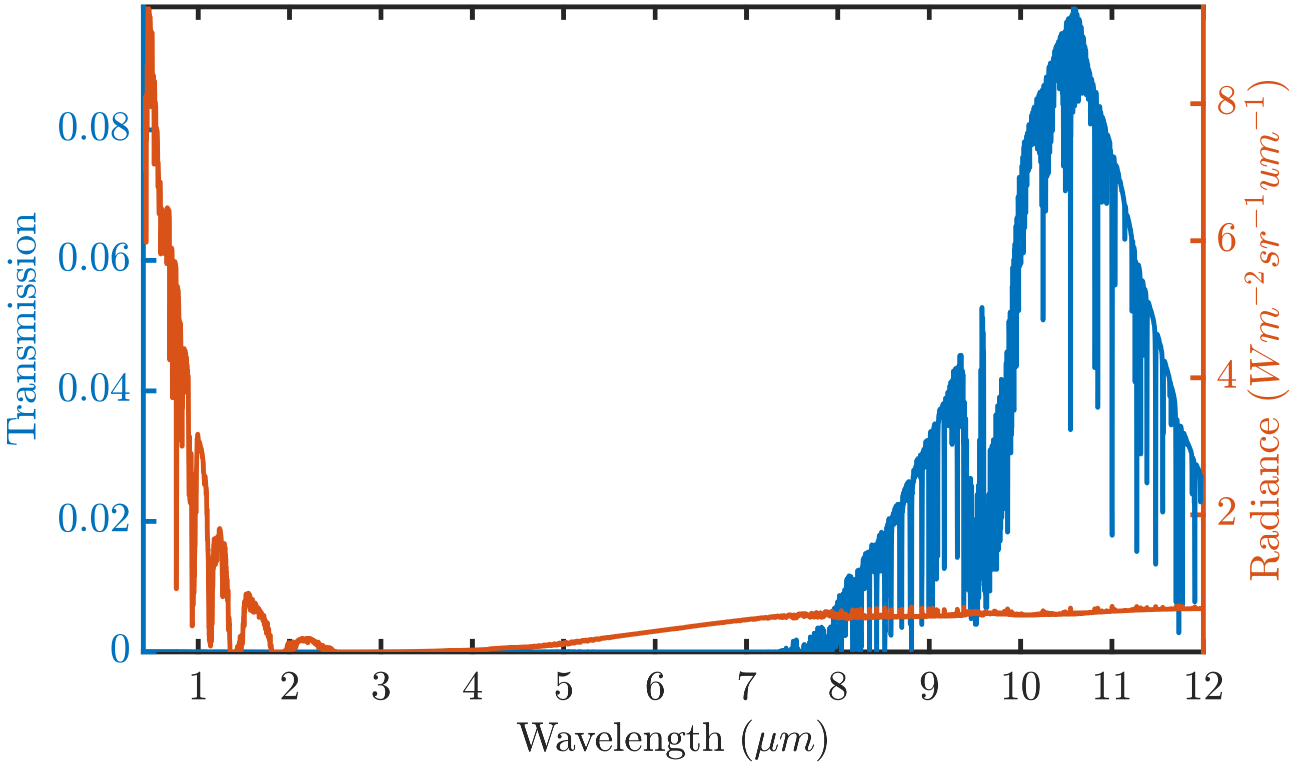
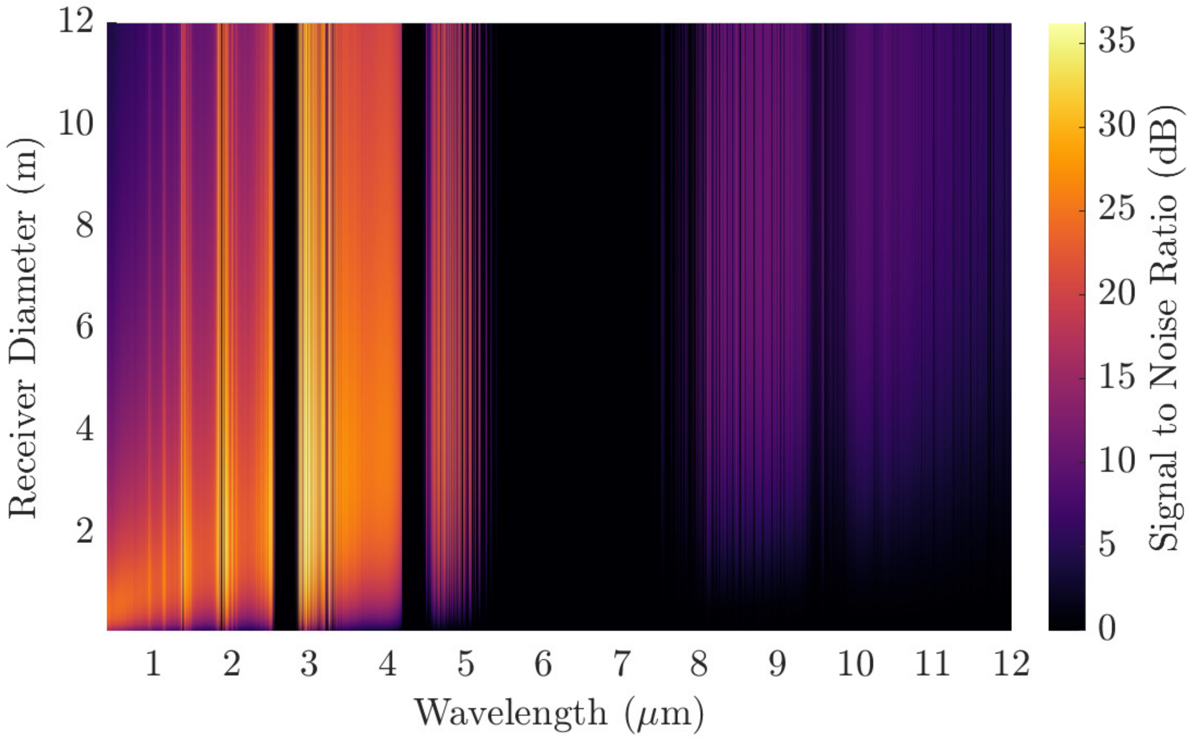


Figure 4.25: Transitivity and radiance plotted as a function of wavelength, for a ground receiver pointed at zenith at 12 pm noon on the winter solstice in Waterford, through a 500 m visibility radiative fog.

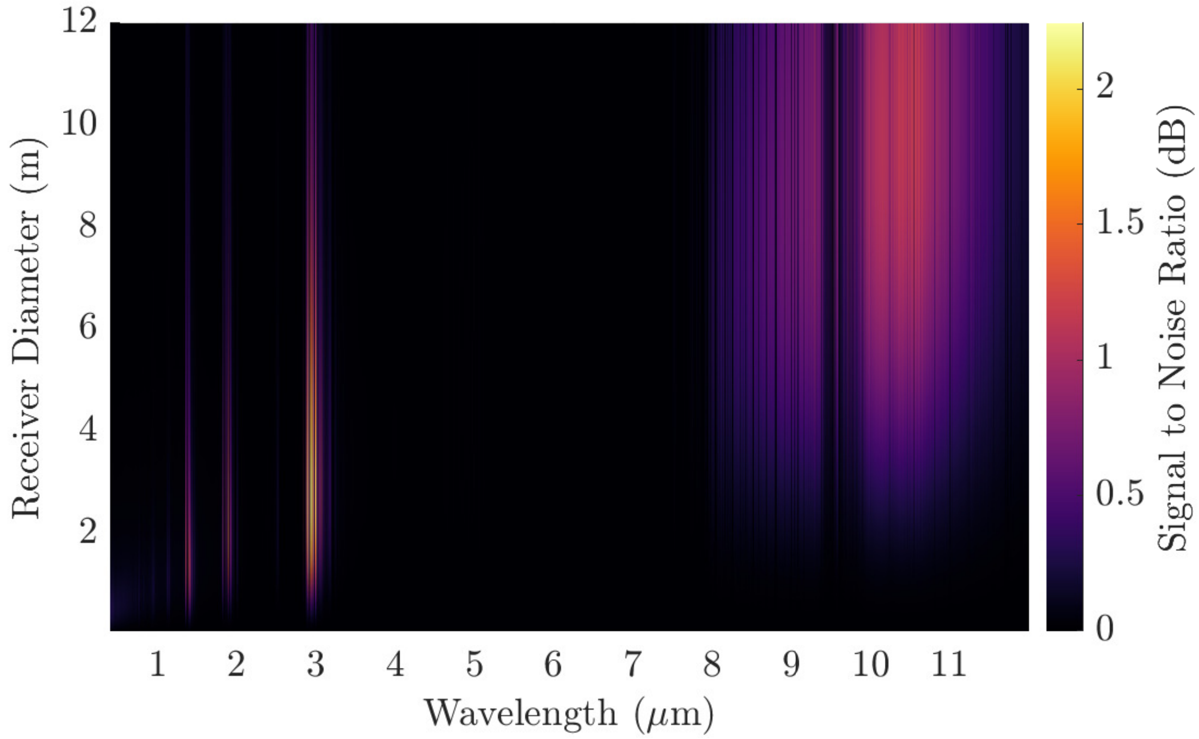
In Figure 4.25, the transmission and radiance are plotted from 400 nm to 12 μm at 12 pm noon on the winter solstice at Waterford, propagating through a 500 m visibility radiative fog. In this plot, the superiority of the LWIR is even more evident. Relative to the LWIR, the other wavelength regions have almost zero transmission. It would seems obvious to conclude that the LWIR is the best region for QKD through adverse weather conditions but further investigation is warranted before such assumptions can be made. The signal to noise ratio and secret key rate must be calculated.

In Figure 4.26, the signal to noise ratio (dB) in Waterford through a) 5 km visibility haze and b) 500 m visibility fog, is plotted using a 3D surface plot for a range of receiver diameters and wavelengths when the initial beam waist is 35 cm and all other parameters are listed in tables 4.1 and 4.2. The 35 cm initial beam waist was chosen to help improve the channel efficiency and increase the chance of the signal getting through the adverse weather conditions. Despite the advantages of the LWIR wavelengths propagating through adverse weather, the LWIR has a significant reduction in signal to noise ratio in comparison to NIR, SIWR and MWIR.

The resulting signal to noise ratio for the condition of light haze is presented in Figure 4.26 (a), where it is evident that the MWIR has significantly better signal to noise ratio then the other regions, even after the SNR is converted to dB. This might seem surprising considering how low



(a)



(b)

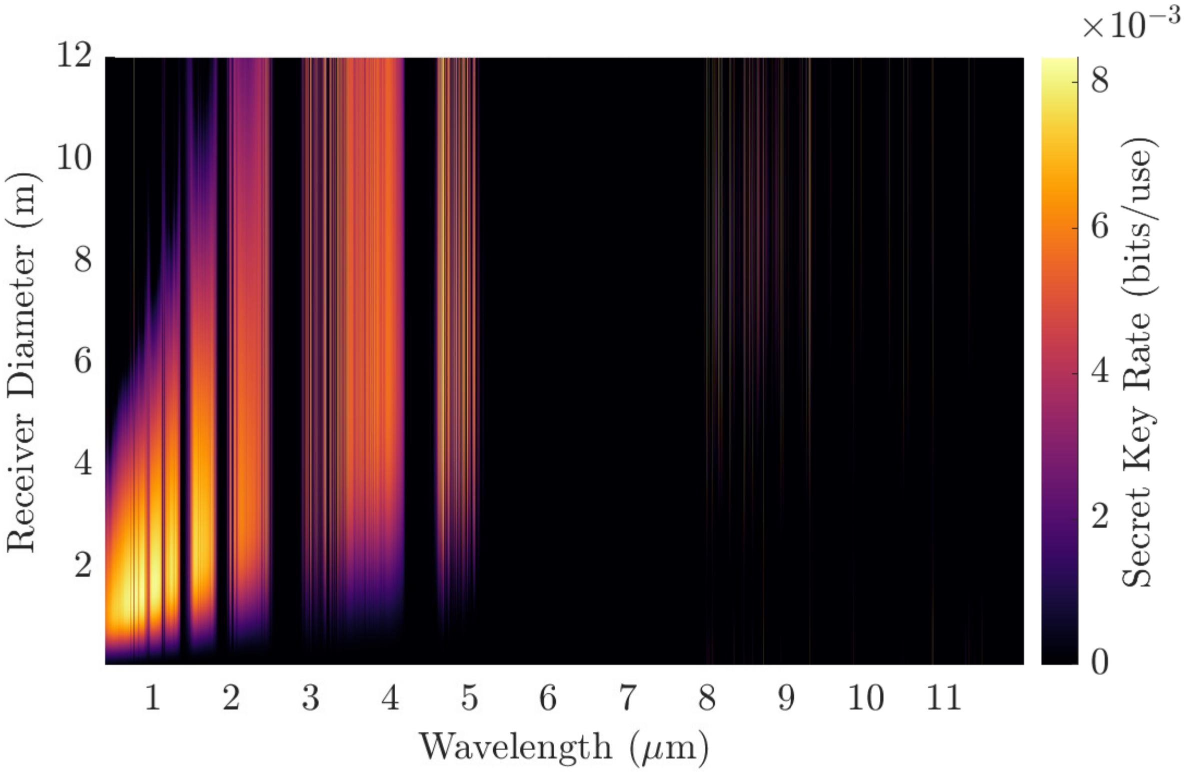
Figure 4.26: 3D surface plot representing the signal to noise ratio (dB) in Waterford through a) 5 km visibility haze and b) 500 m visibility fog, for a range of receiver diameters and wavelengths when the initial beam waist is 35 cm and all other parameters are listed in tables 4.1 and 4.2.

the transmittance is in the MWIR but this can be largely be explained by the low radiance in the MWIR. As noted earlier, the signal to noise ratio is more sensitive to differences in spectral radiance than difference in transmittance. However, the results for signal to noise ratio through dense fog in Figure 4.26 b) seem even more surprising given the huge difference in percentage transmission between the LWIR and all other regions as shown in Figure 4.25. Although there are wavelengths in LWIR that have a higher signal to noise than almost every other wavelength, there is also a higher SNR channel near 3 μm. While this is an interesting result which will be explored in greater detail later in this section, for QKD it is more important to focus on the secret key rate, which is shown for both low visibility conditions is shown in Figure 4.27.

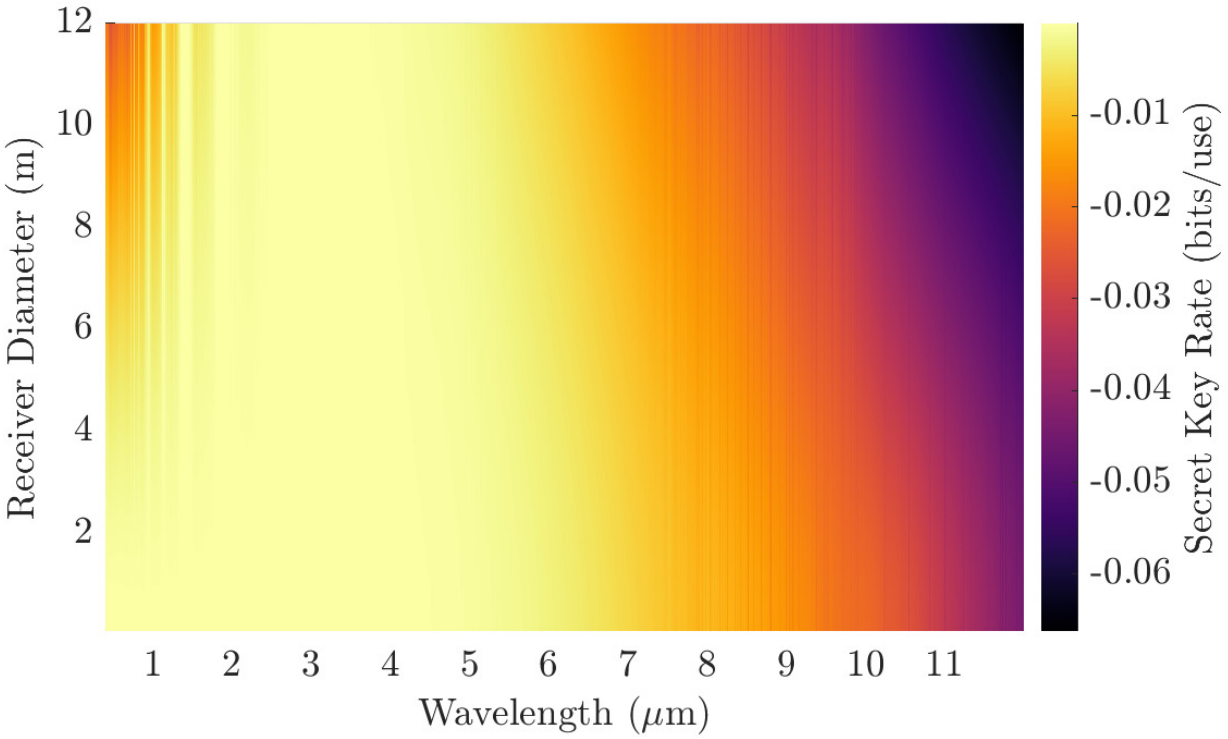
Figure 4.27 (a) shows the secret key rate through light haze and demonstrates that the advantages of LWIR propagation, don't necessarily translate to QKD. It is interesting to note that the best secret key rates generated in haze are obtained using small wavelengths and small receiver sizes. Similarly, in Figure 4.27 b), the secret key rate is determined through dense radiative fog and the results are not as expected. The superior transmission of the LWIR yields some of the highest signal to noise ratios but this does not translate to secret key rate, where the LWIR is actually the worst-performing region. This is a seemingly bizarre result and to properly understand why this occurs, some of the competing parameters must be investigated. Three aerosol models are considered, rural aerosols, haze and fog, each of which is compared side by side using four important parameters. The channel efficiency, the background noise, the signal to noise ratio and the secret key rate. Each parameter has its own colour scale, which is used in each of the conditions.

In Figure 4.28, the channel efficiency is plotted as a 3D surface plot for a range of receiver diameters and wavelengths for each of the atmospheric scenarios. As expected, the rural aerosols typically found in Waterford yield the best channel efficiency. It should be noted that the rural data set is the same one used to generate Figure 4.1 and so it also includes a cirrus cloud model. The haze reduces the channel efficiency significantly but the same channels emerge. The behaviour of the model is pretty similar for the rural and haze scenarios but the fog scenario is quite distinct. The channel efficiency in fog is very low and relative to the other scenarios it is almost negligible. As all three plots in Figure 4.28 are on the same colour scale, the fog plot is black everywhere except for a band between 10 μm and 11 μm due to the peak in transmission, where a faint purple section is visible. Even though the LWIR region has higher transmission through fog, the overall transmission is still very low and not enough to overcome the diffraction losses that dominate the channel efficiency. However, the channel efficiency is still highest in the LWIR when propagating through fog as long as large receivers are used.

In Figure 4.29, the background probability is plotted for each atmospheric scenario. Recall from equation 4.1 that the background probability is the probability of a noise photon entering the detector and it is a combination of N_b, the number of noise photons entering the field stop



(a)



(b)

Figure 4.27: 3D surface plot representing the secret key rate in Waterford through a) 5 km visibility haze and b) 500 m visibility fog, for a range of receiver diameters and wavelengths when the initial beam waist is 35 cm and all other parameters are listed in tables 4.1 and 4.2.

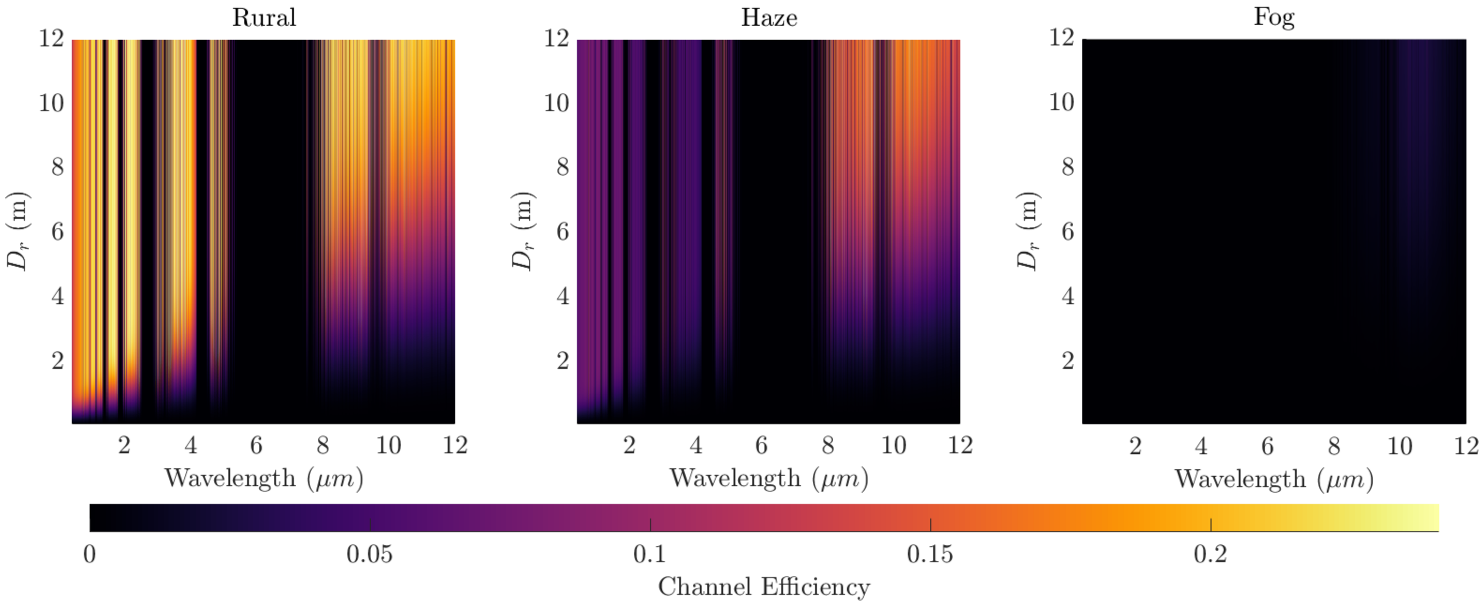


Figure 4.28: 3D surface plot representing the channel efficiency in Waterford through a) rural aerosols, b) light haze and c) dense radiation fog, for a range of receiver diameters and wavelengths when the initial beam waist is 35 cm.

given by equation 3.25, and the detector dark count rate. As discussed earlier in this chapter, the number of photons entering the field stop, and hence the background probability, depends on a number of competing variables such as wavelength, receiver size, spectral radiance and field stop field of view. If all other variables are kept constant, a lower background probability means higher performance in terms of signal to noise ratio and secret key rate. Interestingly, the background probability tends to increase as the visibility is decreased from typical rural conditions, through haze and into dense fog. This is due to an increased scattering of solar and terrestrial radiation, the latter being more significant at the longer end of the wavelength spectrum.

The channel efficiency and the background probability are the two most important equations for understanding signal to noise ratio and secret key rate generation. As already shown, these parameters are determined by a combination of competing variables which makes secret key rate calculations complex. As demonstrated earlier using the MWIR surface plots, the background probability tends to have a larger effect on the signal to noise ratio than it does on secret key rate. Similarly, the channel efficiency tends to have more effect on the secret key rate than it does on the signal to noise ratio. In Figure 4.30, the signal to noise ratio (dB) is compared for each of the atmospheric conditions. As expected, the signal to noise ratio decreases as the visibility decreases due to a reduction in channel efficiency and an increase in background probability. These plots also help to understand the different performance of each wavelength region. A higher channel efficiency for the LWIR wavelengths in haze is counteracted by a high background probability, resulting in a poorer signal to noise ratio. In contrast a weaker channel efficiency in the SWIR and MWIR regions are compensated by a low background probability

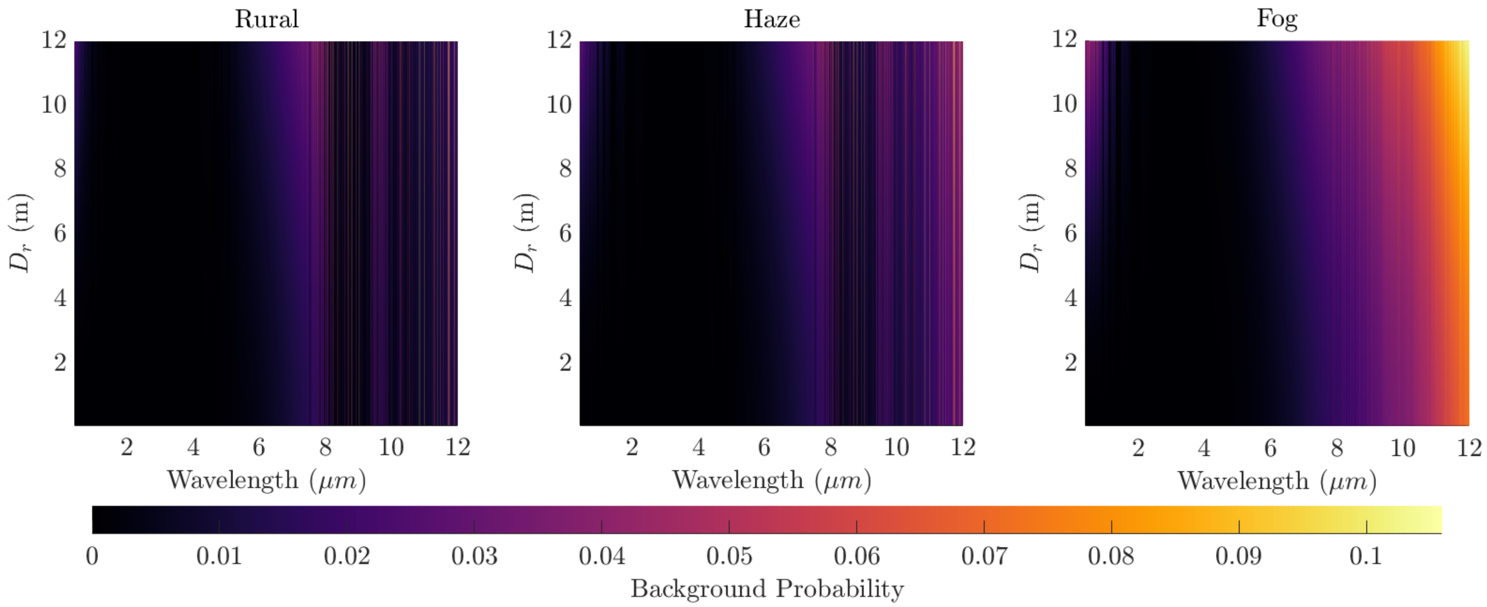


Figure 4.29: 3D surface plot representing the background probability in Waterford through a) rural aerosols, b) light haze and c) dense radiation fog, for a range of receiver diameters and wavelengths when the initial beam waist is 35 cm.

which results in a high signal to noise ratio across each region. Due to the colour scale, there is not much information to be gained looking at the fog plot in Figure 4.30, so instead see Figure 4.26 b) where the same data is plotted with its own colour gradient. From that plot, it is clear the LWIR achieves significantly higher signal to noise than all other regions, with the exception of a channel near 3 μm. This is interesting as the LWIR has by far the highest background probability in the presence of fog, so it seems to contradict the relationship previously established between signal to noise ratio and background probability. It turns out that when the channel efficiency is high, the signal to noise ratio is inversely proportional to the background probability as discussed already, but when the channel efficiency is low, the relationship breaks down. When the channel efficiency is as low as it is in the presence of dense fog, then small variations in channel efficiency tend to have a much bigger effect on signal to noise ratio. As such, the relative higher channel efficiency in some of the LWIR wavelengths is enough to overcome the higher background probability and produce a higher signal to noise ratio than other wavelengths.

Now that the signal to noise ratios dependence on channel efficiency and background probability is understood, a similar breakdown of secret key rate is necessary. In Figure 4.31, the secret key rate (bits/use) is compared for each of the atmospheric conditions. As noted earlier, the channel efficiency tends to have more control over the value of the secret key rate than the background probability. This remains true provided the channel efficiency is relatively high and the background probability is relatively low. However, in conditions of low visibility such as haze and fog, the channel efficiency is reduced while the background probability is increased so background probability tends to have a higher correlation with poor secret key rates compared

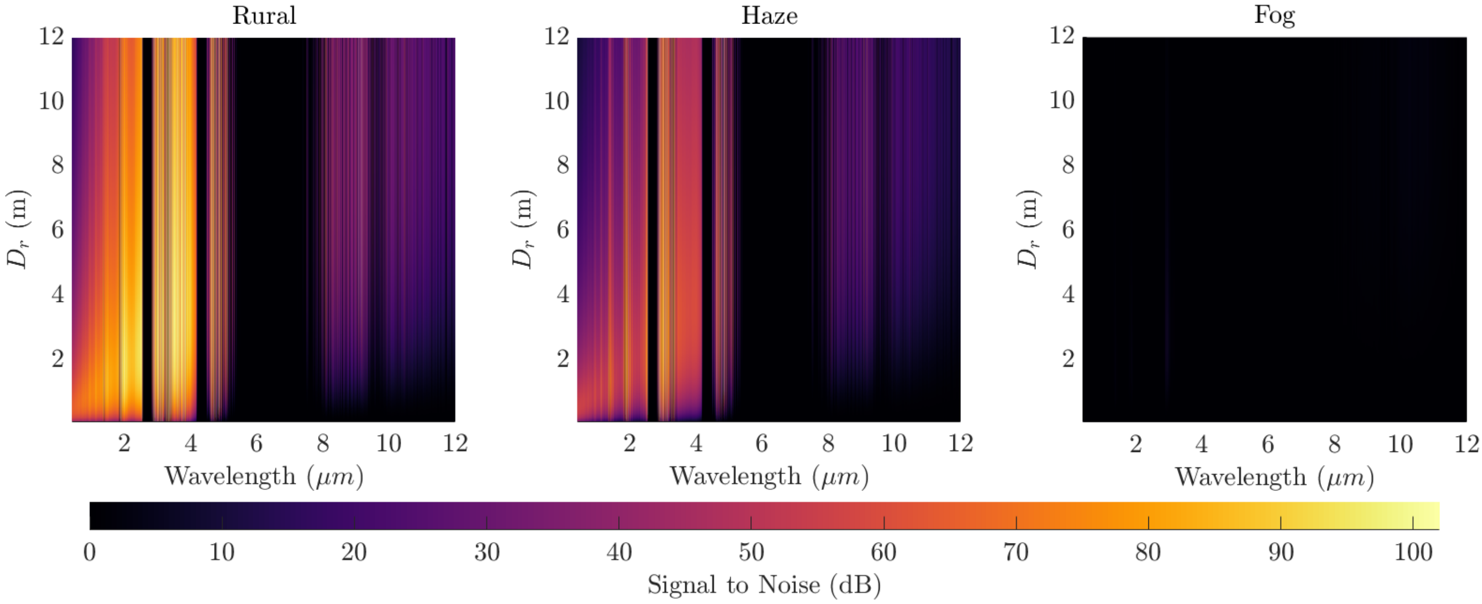


Figure 4.30: 3D surface plot representing the signal to noise ratio (dB) in Waterford through a) rural aerosols, b) light haze and c) dense radiation fog, for a range of receiver diameters and wavelengths when the initial beam waist is 35 cm and all other parameters are listed in tables 4.1 and 4.2.

to performance in normal conditions. This effect can clearly be seen by comparing the secret key rate in haze with the equivalent channel efficiency and background probability. Despite the LWIR having the highest channel efficiency, it also has the highest background probability and thus achieves the lowest resulting secret key rate. This effect is even more pronounced for the results modelling fog, which is easier to visualise looking at 4.27 (b) where the same data is plotted with its own colour scale. Despite the LWIR having a higher channel efficiency, (see Figure 4.28 (b)) and a higher signal to noise ratio, (see Figure 4.26 (b)), it has by far the lowest secret key rate, see (Figure 4.27 (b)). This is a result of the extremely high background noise dominating the performance of the secret key rate when the channel efficiency is low.

Although quantum communication through fog and haze is interesting to study, especially at longer wavelengths in the LWIR, rain and cloud cover are much more typical atmospheric conditions for Waterford. MODTRAN has a number of cloud models but most are completely attenuating so the bulk propagation characteristics through rain and clouds are represented here by the drizzle rain cloud model. The transmittance and radiance are plotted together in Figure 4.32. Once again, the transmittance peaks in the LWIR but the signal is still almost completely attenuated and the radiance dominates. Therefore the system is incapable of generating a positive secret key rate through drizzle rain clouds, as shown in Figure 4.33.

To conclude this section, decreasing visibility tends to negatively impact secret key rate in two ways, firstly by absorbing and scattering signal photons and secondly by scattering background light from external sources thus yielding even higher spectral radiance at the receiver. As a

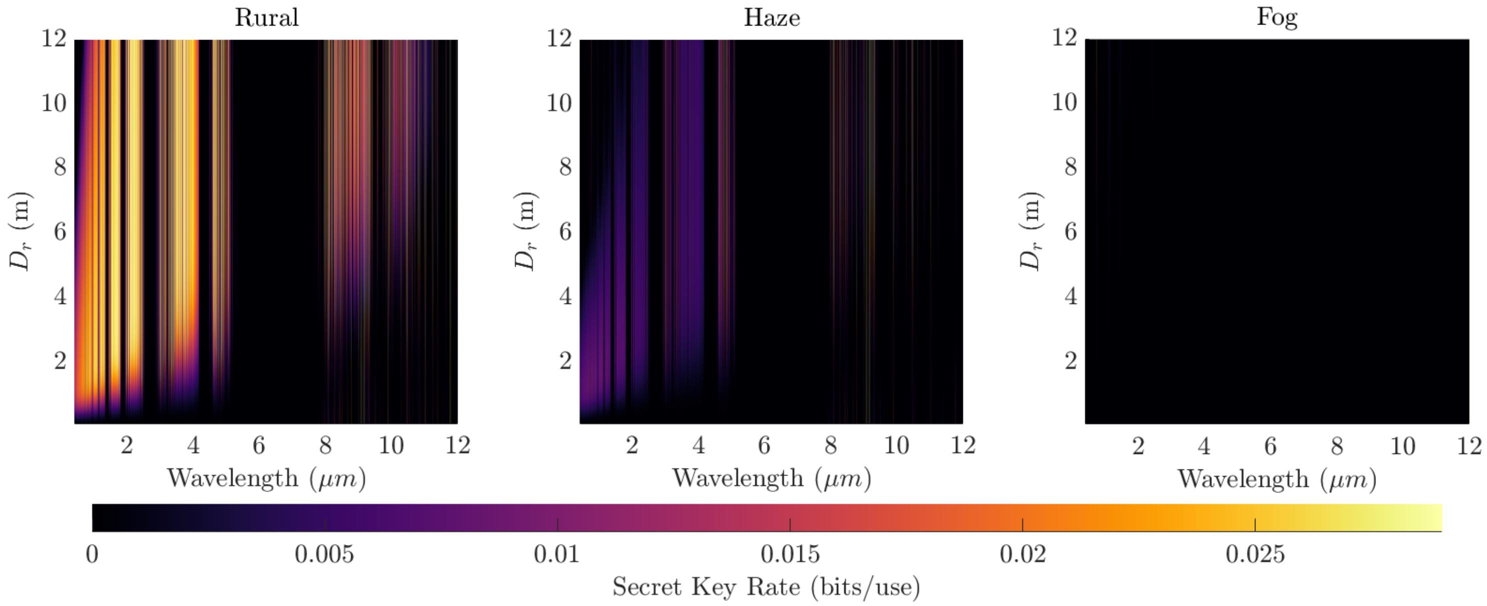


Figure 4.31: 3D surface plot representing the secret key rate in Waterford through a) rural aerosols, b) light haze and c) dense radiation fog, for a range of receiver diameters and wavelengths when the initial beam waist is 35 cm and all other parameters are listed in tables 4.1 and 4.2

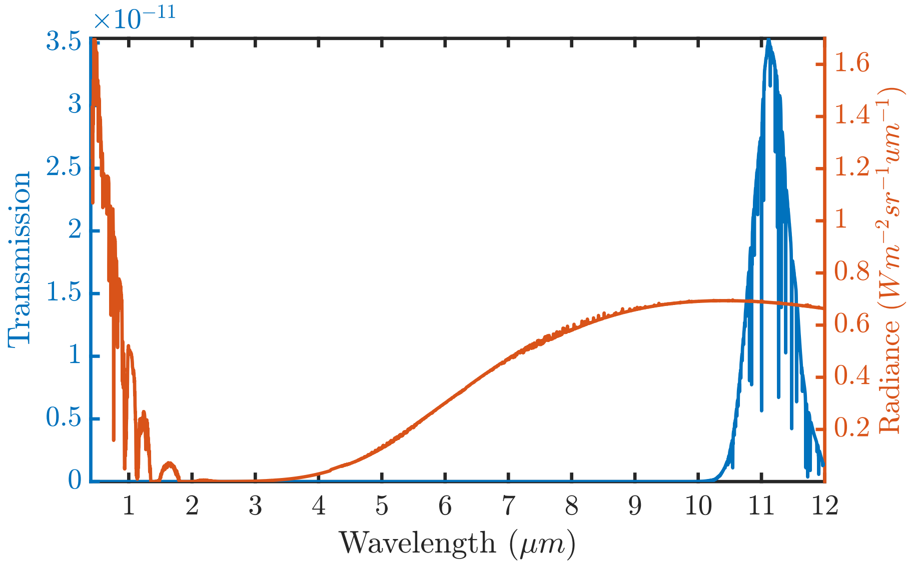


Figure 4.32: Transitivity and radiance plotted as a function of wavelength, for a ground receiver pointed at zenith at 12 pm noon on the winter solstice in Waterford, through drizzle rain clouds

result, stringent spatial filtering is required to achieve a positive secret key rate in adverse conditions. The visible, NIR and SWIR wavelengths tend to do well in haze due to their low spot size which allows tight spatial filtering, as shown in Figure 4.27. Despite the superior propagation of LWIR through fog and haze, the additional noise combined with the larger spot size limits QKD performance. Figure 4.27 (b) and Figure 4.33 highlight the difficulty of achieving global quantum communications as none of the wavelengths are able to generate a positive secret key rate through fog or light rain.

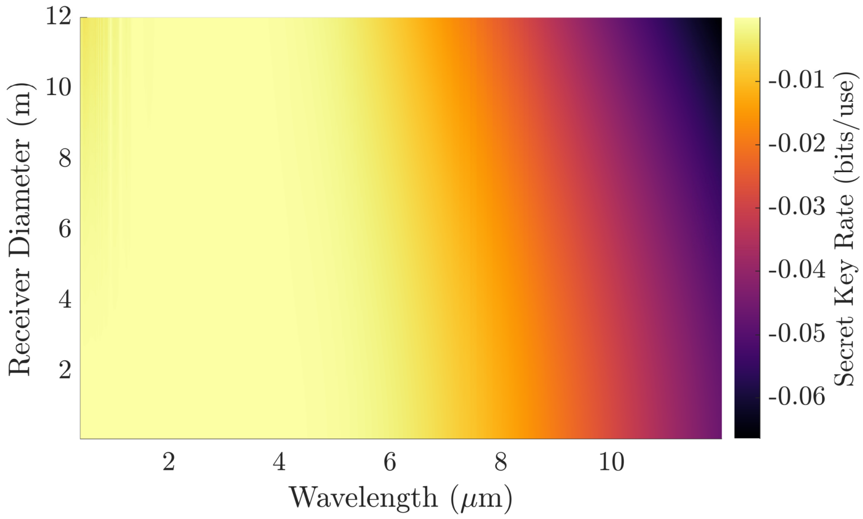


Figure 4.33: Secret Key Rate as a function of wavelength and receiver size, for a ground receiver pointed at zenith at 12 pm noon on the winter solstice in Waterford, through drizzle rain clouds

Chapter 5

Conclusion

The main goal of this thesis was to explore what wavelengths are suitable for practical quantum satellite communications. To this end, the satellite downlink was investigated by developing a channel model and using the BB84 decoy-state quantum key distribution rate as a performance metric. The signal to noise ratio and secret key rate were determined for this protocol for a wide range of wavelengths while considering operation in a broad space of atmospheric, geometric and geographical conditions.

5.1 Summary of Results

Two scenarios were considered, the summer solstice in Tucson Arizona, to represent an ideal location for satellite communication whereas the overcast climate of an Irish winter solstice in Waterford represents a not so ideal location. Tucson's atmosphere was modelled for a completely clear sky and although the transmission is very high, the total radiance is also extremely high, considering the simulation was performed at the daily peak in solar radiation. As a result, Tucson experiences less signal to noise ratio than Waterford due to the huge SNR dependence on total radiation. However, the secret key rate is ultimately determined by signal gain, which is a combination of signal and noise photons, yielding excellent performance for the Tucson scenario. On a relatively clear winter's day with light cirrus clouds, Waterford is capable of yielding high signal to noise ratios and secret key rates due to the low solar radiance. Despite Waterford having a signal to noise advantage, Tucson clearly achieves a significant improvement in secret key rate generation. Additionally, Irish winter skies are often covered by clouds and when more common atmospheric conditions are introduced, satellite communications become very challenging. The results demonstrate the advantages of using Tucson over Waterford as a ground receiver location for quantum satellite communications. They also serve to highlight the differences in optimal wavelength between the two conditions, demonstrating the trade-off between signal gain and background probability. The high spectral radiance in Tucson mandates that smaller wavelengths are used so that tighter spatial filtering can eliminate the excess noise while in Waterford, larger receivers and wavelengths are used to improve the channel efficiency which suffers due to the prevalence of absorption and scattering in this scenario.

There are numerous atmospheric transmission windows across the electromagnetic spectrum but lack of components that operate at longer wavelengths has dissuaded researchers from investigating the potential benefits of wavelengths outside the visible, NIR and SWIR regions. The MWIR and LWIR remain largely unexplored for QKD but advancements in quantum cascade lasers and superconducting nanowire single-photon detectors (SNSPD) enable further research into these alternative wavelengths. Device efficiencies are considered constant across all wavelengths in order to isolate the physics related to the propagation of quantum signals, revealing if it is worthwhile to devout more resources to the development of longer wavelength technology. However, as the wavelength is increased, so too must the component sizes increase to account for the additional free-space beam spread. While the wavelengths can be compared for a given receiver size, to find what wavelengths are applicable to satellite QKD, it makes sense to compare the wavelengths and component sizes together. The initial beam waist has a significant impact on the performance of the system, but the magnitude of the effect is similar for all wavelengths so initially only two cases are considered, 10 cm and 35 cm. It is important to consider wavelength performance directly beside receiver aperture due to interactions between signal photons, noise photons, wavelength and receiver aperture. To this end, a number of 3D surface plots were generated showing wavelength on the x-axis, receiver diameter aperture on the y-axis and the chosen performance metric on the z-axis where a colour scale is used to visualize performance. In this way, the wavelength regions across the spectrum can be directly compared while accounting for different component sizes to determine the best wavelength-receiver combinations. They can also be used to inform researchers who wish to choose the best components for a given wavelength while also serving as a good reference for practical implementation, where the best wavelength can be selected for the component size limitations imposed by each individual use case.

Due to the smaller beam size at the receiver, the visible window is capable of the tightest spatial filtering and can overcome its disadvantage as the window that experiences the highest intensity of solar radiation. Therefore the visible region performs well when the receiver size is small and will be most suitable for component size-limited applications.

In comparison to infrared wavelengths, NIR wavelengths also benefit from having a smaller beam spot size at the receiver. The low diffraction losses compound with high transmittance to produce an efficient channel. However, high solar radiance in the NIR mandates that smaller receivers are used to filter out the excess noise photons which reduce the signal gain and ultimately the secret key rate. The importance of the NIR region is that it enables high secret key rates without requiring huge receivers. Additionally, the ability to implement stringent filtering techniques becomes even more important when operating through adverse weather conditions, which makes shorter wavelengths in the visible and NIR regions most suitable.

The SWIR window has the highest transmittance across the whole spectrum while also experiencing some of the lowest spectral radiance. SWIR wavelengths can suffer more loss from beam spread than those in the visible and NIR regions but if large enough receivers are used, the SWIR has the highest secret key rate performance.

If large transmitters and receivers are implemented then there are pockets of the MWIR region that are capable of achieving secret key rates as high as best SWIR wavelengths. The major benefit of using the MWIR region is the performance through atmospheric turbulence. Longer waves in general perform better in turbulence but some MWIR wavelengths combine this with

low radiance and high transmittance so that if large enough components are used, sections of the MWIR are capable of generating high rates without needing AO correction.
Despite low radiance across the entire LWIR region, longer wavelengths suffer severely from losses due to the size of the beam waist at the receiver. Usable secret key rates are achievable if larger transmitters and receivers are used but there does not seem to be any benefit to using the LWIR region when atmospheric conditions are good. The attraction of LWIR wavelengths is the superior propagation through adverse weather conditions but this benefit does not translate to secret key rate, where the beam spread requires receivers which are so large that they inevitably let in too many noise photons.

For each transmission window there exists a wavelength-receiver combination that maximises secret key rate for the 10 cm and 35 cm initial beam waists respectively. The secret key rate can be improved further while decreasing the receiver size by optimizing the initial beam waist. A single wavelength is taken from each transmission window and the receiver aperture diameter is optimized alongside the initial beam waist to find the combination of wavelength, initial beam waist and receiver aperture, that maximises secret key rate in each region. This allows the best-case scenario for each wavelength region to be compared side by side to determine what regions achieve the best performance. This is perhaps best demonstrated by plotting each on a 2D graph with coherence length on the x-axis and the secret key rate on the y-axis, indicating the performance as turbulence is varied. The results show that when turbulence is low or equivalently compensated by the 200 Hz AO unit, the SWIR and MWIR offer the best performance. When the turbulence strength is increased, or when the turbulence is uncompensated, the MWIR performs significantly better. Indeed, the MWIR shows so much resilience against the effects of turbulence that even when the distorted MWIR wavefront is uncompensated by AO, it outperforms the AO corrected wavefronts of the visible and LWIR wavelengths. This suggests that the MWIR could be used in place of an adaptive optics unit to implement high-performance QKD. However, the MWIR requires large transmitters and receivers to obtain these values which may make operating at these wavelengths impractical.

It is now understood that maximising secret key rate requires the use of large transmitters and receivers but practical scenarios place size limitations on the components used. Therefore it is important not just to determine what wavelengths produce the highest performance when the ideal component sizes are available, but also what wavelengths produce the highest performance when the component sizes are limited. In Tucson and Waterford, for 10 cm and 35 cm initial beam waists, the best wavelengths are determined for each receiver size ranging from 0.25 m to 12 m. When w_0 is 10 cm, visible wavelengths tend to produce the highest secret key rates for lower D_r values due to the smaller spot size at the receiver. As D_r increases the optimal λ transition to the NIR region and at 3 m the NIR channel at 0.867 μm achieves the best QKD performance. Longer NIR wavelengths become more suitable as D_r is increased further but after 6 m the SWIR region dominates, reaching a maximum secret key rate of

0.0284 bits/use at 2.134 μm. This rate requires a massive 11 m receiver which is probably unnecessary considering a rate of 0.0262 bits/use is obtainable using the channel at 1.556 μm and a 6 m receiver. So an 83% increase in D_r only yields an 8.4% improvement in secret key rate. When w_0 is 35 cm, visible wavelengths still yield the best performance for lower D_r sizes. The larger w_0 serves to decrease the amount of beam spread which means that the NIR wavelengths start to outperform the visible wavelengths at smaller D_r values. At 1 m the 0.867 μm NIR wavelength is optimum. When D_r is small any increase will yield dramatic improvements in secret key rate and optimum wavelength but if a larger w_0 is used, the effect of increasing D_r is far less effective. The commonly used channel at 1.556 μm achieves a secret key rate of 0.0271 bits/use using only a 2 m receiver. The secret key rate is close to its maximum value using the channel at 2.135 μm and a 3 m receiver and although higher secret key rates can be obtained by increasing the D_r beyond 3 m, it does not yield a significant performance improvement. Considering that an abundance of optical devices are already optimised for the high-performance channel at 1.556 μm, it seems likely that it is the most practical channel for high-performance satellite QKD despite longer SWIR and MWIR channels achieving slightly higher secret key rates. However smaller component size limitations, such has those on a CubeSat, will mandate that visible or NIR wavelengths are used to maximise secret key rate.

Finally, the transmission windows are compared in conditions of low visibility such as haze, fog and rain. Reduced visibility has two effects on secret key rate, first, it absorbs and scatters signal photons, and second, it scatters background light from external sources resulting in even higher radiance at the receiver. In order to attain a positive secret key rate in unfavourable atmospheric conditions, tight spatial filtering is required. As illustrated in chapter 4, visible, NIR, and SWIR wavelengths perform well in haze because of their small spot size, which allows for fine spatial filtering. Despite the LWIR's greater propagation through fog and haze, LWIR QKD performance is limited by increased background noise due to the larger receivers necessary to capture a bigger spot size.

This thesis has documented the QKD performance of different transmission windows across the electromagnetic spectrum and determined which wavelengths are most optimal in a range of conditions. The key takeaway is that there is no best wavelength but instead, each region has its own advantages and drawbacks and the future of QKD could be shared by a number of wavelengths. Indeed, the most optimal wavelength for a given use case is determined by many variables and to achieve the very best performance, the channel should be modelled to uncover what conditions produce the highest secret key rates. This work serves as a quick reference to determine what components and wavelengths are optimal for a given use case, by directly comparing the performance of the best wavelengths in each region, operating in a variety of conditions. If the application is limited by small components then the visible and NIR regions offer the best performance. If slightly larger components can be used, then the SWIR channels near 1.556 μm offer excellent performance without requiring huge components, although even higher secret key rates can be achieved if larger components are used to enable the high-performance channels at 2.134 μm and 2.141 μm in Tucson and Waterford respectively. If operating in conditions of strong turbulence or if an adaptive optics unit is unavailable, then the MWIR offers great performance but requires larger transmitters and receivers to account for the additional beam spread. Although a use-case for the LWIR has not been demonstrated in this work, perhaps the region is better suited to short-range terrestrial propagation, where the reduction in attenuation through low visibility conditions and excellent propagation through turbulence can offset the additional beam spread.

5.2 Future Work

The focus of this work has been on the downlink satellite scenario to support the abundance of ongoing experiential work to achieve daytime satellite quantum key distribution. The uplink presents a much more challenging scenario for implementing QKD due to the effects of turbulence which influence the beam while it is still small, resulting in significant loss at the receiver. One of the aims of this research was to investigate the potential advantages of some longer wavelengths in the MWIR and LWIR that have traditionally been overlooked due to a lack of devices. As extensively explored in this work, the MWIR and LWIR are substantially more resilient to the effects of turbulence and could overcome much of the uplink loss. Additionally, there is far less solar radiation in the MWIR and LWIR in comparison to smaller wavelengths, which is the dominant source of background noise, especially for satellite-based receivers. It is important to note that the size of the receiver on the satellite payload is under much stricter size limitations than an equivalent ground station and may struggle to capture the power of a larger beam waist. Future work should be focused on implementing an uplink scenario to test this hypothesis and determine if longer wavelengths can enable uplink QKD.

This research could be improved further by considering angles other than those at zenith and by adding an Acquisition, Tracking and Pointing (ATP) system to see how such a system is influenced by wavelength selection. The altitude of the satellite is an important variable and also requires further investigation. Additionally, the implications of wavelength choice on alternative QKD protocols could be investigated, to determine what wavelengths are most suitable for Entanglement or Continuous Variable (CV) QKD protocols. Finally, perhaps the huge improvement in signal to noise ratio at the MWIR region could be exploited by a novel QKD protocol which seeks to obtain security by minimising background noise.

Bibliography

[1] Alko R Meijer et al. *Algebra for Cryptologists*. Springer, 2016.

[2] Peter W Shor. “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer”. In: *SIAM review* 41.2 (1999), pp. 303–332.

[3] Peter W Shor. “Algorithms for quantum computation: discrete logarithms and factoring”. In: *Proceedings 35th annual symposium on foundations of computer science*. Ieee. 1994, pp. 124–134.

[4] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge University Press, 2000.

[5] Lieven MK Vandersypen et al. “Experimental realization of Shor’s quantum factoring algorithm using nuclear magnetic resonance”. In: *Nature* 414.6866 (2001), p. 883.

[6] Charles H Bennett and Gilles Brassard. “Quantum cryptography: Public key distribution and coin tossing”. In: *arXiv preprint arXiv:2003.06557* (2020).

[7] William K Wootters and Wojciech H Zurek. “A single quantum cannot be cloned”. In: *Nature* 299.5886 (1982), pp. 802–803.

[8] Valerio Scarani et al. “The security of practical quantum key distribution”. In: *Reviews of modern physics* 81.3 (2009), p. 1301.

[9] Artur K Ekert. “Quantum cryptography based on Bell’s theorem”. In: *Physical review letters* 67.6 (1991), p. 661.

[10] Charles H Bennett, Gilles Brassard, and N David Mermin. “Quantum cryptography without Bell’s theorem”. In: *Physical review letters* 68.5 (1992), p. 557.

[11] Charles H Bennett. “Quantum cryptography using any two nonorthogonal states”. In: *Physical review letters* 68.21 (1992), p. 3121.

[12] Dagmar Bruß. “Optimal eavesdropping in quantum cryptography with six states”. In: *Physical Review Letters* 81.14 (1998), p. 3018.

[13] Timothy C Ralph. “Security of continuous-variable quantum cryptography”. In: *Physical Review A* 62.6 (2000), p. 062306.

[14] Henning Weier et al. “Quantum eavesdropping without interception: an attack exploiting the dead time of single-photon detectors”. In: *New Journal of Physics* 13.7 (2011), p. 073024.

[15] ZL Yuan, James F Dynes, and Andrew J Shields. “Avoiding the blinding attack in QKD”. In: *Nature Photonics* 4.12 (2010), pp. 800–801.

[16] Yan-Lin Tang et al. “Source attack of decoy-state quantum key distribution using phase information”. In: *Physical Review A* 88.2 (2013), p. 022308.

[17] Won-Young Hwang. “Quantum key distribution with high loss: toward global secure communication”. In: *Physical Review Letters* 91.5 (2003), p. 057901.

[18] Hoi-Kwong Lo, Marcos Curty, and Bing Qi. “Measurement-device-independent quantum key distribution”. In: *Physical review letters* 108.13 (2012), p. 130503.

[19] Yan-Lin Tang et al. “Measurement-device-independent quantum key distribution over untrustful metropolitan network”. In: *Physical Review X* 6.1 (2016), p. 011024.

[20] Eleni Diamanti et al. “Practical challenges in quantum key distribution”. In: *npj Quantum Information* 2.1 (2016), pp. 1–12.

[21] Noson S Yanofsky and Mirco A Mannucci. *Quantum computing for computer scientists*. 2008.

[22] Jonathan A Jones and Dieter Jaksch. *Quantum information, computation and communication*. Cambridge University Press, 2012.

[23] H-J Briegel et al. “Quantum repeaters: the role of imperfect local operations in quantum communication”. In: *Physical Review Letters* 81.26 (1998), p. 5932.

[24] Qiao Ruihong and Meng Ying. “Research progress of quantum repeaters”. In: *Journal of Physics: Conference Series*. Vol. 1237. 5. IOP Publishing. 2019, p. 052032.

[25] Purva Sharma et al. “Quantum key distribution secured optical networks: a survey”. In: *IEEE Open Journal of the Communications Society* (2021).

[26] Chip Elliott et al. “Current status of the DARPA quantum network”. In: *Quantum Information and computation III*. Vol. 5815. International Society for Optics and Photonics. 2005, pp. 138–149.

[27] Momtchil Peev et al. “The SECOQC quantum key distribution network in Vienna”. In: *New Journal of Physics* 11.7 (2009), p. 075001.

[28] ZL Yuan and AJ Shields. “Continuous operation of a one-way quantum key distribution system over installed telecom fibre”. In: *Optics express* 13.2 (2005), pp. 660–665.

[29] Rachel Courtland. “China’s 2,000-km quantum link is almost complete [News]”. In: *IEEE Spectrum* 53.11 (2016), pp. 11–12.

[30] M Minder et al. “Experimental quantum key distribution beyond the repeaterless secret key capacity”. In: *Nature Photonics* 13.5 (2019), pp. 334–338.

[31] Jiu-Peng Chen et al. “Twin-field quantum key distribution over a 511 km optical fibre linking two distant metropolitan areas”. In: *Nature Photonics* (2021), pp. 1–6.

[32] Shuang Wang et al. “Twin-field quantum key distribution over 830-km fibre”. In: *Nature Photonics* 16.2 (2022), pp. 154–161.

[33] Sheng-Kai Liao et al. “Satellite-to-ground quantum key distribution”. In: *Nature* 549.7670 (2017), pp. 43–47.

[34] Juan Yin et al. “Satellite-based entanglement distribution over 1200 kilometers”. In: *Science* 356.6343 (2017), pp. 1140–1144.

[35] Jian-Yu Wang et al. “Direct and full-scale experimental verifications towards ground–satellite quantum key distribution”. In: *nature photonics* 7.5 (2013), pp. 387–393.

[36] JP Bourgoin et al. “A comprehensive design and performance analysis of low Earth orbit satellite quantum communication”. In: *New Journal of Physics* 15.2 (2013), p. 023006.

[37] Giuseppe Vallone et al. “Experimental satellite quantum communications”. In: *Physical Review Letters* 115.4 (2015), p. 040502.

[38] Sheng-Kai Liao et al. “Satellite-to-ground quantum key distribution”. In: *Nature* 549.7670 (2017), pp. 43–47.

[39] Hideki Takenaka et al. “Satellite-to-ground quantum-limited communication using a 50-kg-class microsatellite”. In: *Nature photonics* 11.8 (2017), pp. 502–508.

[40] Stefano Pirandola. “Satellite quantum communications: Fundamental bounds and practical security”. In: *Physical Review Research* 3.2 (2021), p. 023130.

[41] Stefano Pirandola et al. “Fundamental limits of repeaterless quantum communications”. In: *Nature communications* 8.1 (2017), pp. 1–15.

[42] Robert Bedington, Juan Miguel Arrazola, and Alexander Ling. “Progress in satellite quantum key distribution”. In: *npj Quantum Information* 3.1 (2017), pp. 1–13.

[43] Miao Er-long et al. “Background noise of satellite-to-ground quantum key distribution”. In: *New Journal of Physics* 7.1 (2005), p. 215.

[44] Andrea Tomaello et al. “Link budget and background noise for satellite quantum key distribution”. In: *Advances in Space Research* 47.5 (2011), pp. 802–810.

[45] Hemani Kaushal, VK Jain, and Subrat Kar. *Free space optical communication*. Springer, 2017.

[46] Mark T Gruneisen et al. “Adaptive-Optics-Enabled Quantum Communication: A Technique for Daytime Space-To-Earth Links”. In: *Physical Review Applied* 16.1 (2021), p. 014067.

[47] David A Rockwell and G Stephen Mecherle. “Wavelength selection for optical wireless communications systems”. In: *Optical Wireless Communications IV*. Vol. 4530. International Society for Optics and Photonics. 2001, pp. 27–35.

[48] D Vasylyev, AA Semenov, and W Vogel. “Atmospheric quantum channels with weak and strong turbulence”. In: *Physical review letters* 117.9 (2016), p. 090501.

[49] Sheng-Kai Liao et al. “Long-distance free-space quantum key distribution in daylight towards inter-satellite communication”. In: *Nature Photonics* 11.8 (2017), pp. 509–513.

[50] Eduardo Villaseñor et al. “Atmospheric effects on satellite-to-ground quantum key distribution using coherent states”. In: *arXiv preprint arXiv:2005.10465* (2020).

[51] M Avesani et al. “Full daylight quantum-key-distribution at 1550 nm enabled by integrated silicon photonics”. In: *npj Quantum Information* 7.1 (2021), pp. 1–8.

[52] R Nicholas Lanning et al. “Quantum Communication Over Atmospheric Channels–A Framework for Optimizing Wavelength and Filtering”. In: *arXiv preprint arXiv:2104.10276* (2021).

[53] Erik Kerstel et al. “Nanobob: a CubeSat mission concept for quantum communication experiments in an uplink configuration”. In: *EPJ Quantum Technology* 5.1 (2018), p. 6.

[54] Jean-Philippe Bourgoin et al. “Free-space quantum key distribution to a moving receiver”. In: *Optics express* 23.26 (2015), pp. 33437–33447.

[55] R Nicholas Lanning et al. “Quantum Communication Over Atmospheric Channels–A Framework for Optimizing Wavelength and Filtering”. In: *arXiv preprint arXiv:2104.10276* (2021).

[56] THIERRY Aellen et al. “Feasibility study of free-space quantum key distribution in the mid-infrared”. In: *Quantum Information and Computation* 8.1&2 (2008), pp. 0001–0011.

[57] Ziqing Wang, Robert Malaney, and Jonathan Green. “Inter-satellite quantum key distribution at terahertz frequencies”. In: *ICC 2019-2019 IEEE International Conference on Communications (ICC)*. IEEE. 2019, pp. 1–7.

[58] Andrew Pavelchek et al. “Long-wave infrared (10-micron) free-space optical communication system”. In: *Free-Space Laser Communication and Active Laser Illumination III*. Vol. 5160. International Society for Optics and Photonics. 2004, pp. 247–252.

[59] Maha Achour. “Free-space optics wavelength selection: 10 μm versus shorter wavelengths”. In: *journal of optical networking* 2.6 (2003), pp. 127–143.

[60] Federico Capasso et al. “New frontiers in quantum cascade lasers and applications”. In: *IEEE Journal of selected topics in quantum electronics* 6.6 (2000), pp. 931–947.

[61] R Martini et al. “Free-space optical transmission of multimedia satellite data streams using mid-infrared quantum cascade lasers”. In: *Electronics Letters* 38.4 (2002), pp. 181–183.

[62] CP Colvero et al. “Experimental comparison between far-and near-infrared wavelengths in free-space optical systems”. In: *Microwave and optical technology letters* 46.4 (2005), pp. 319–323.

[63] Xiaodan Pang et al. “Free-Space Communications Enabled by Quantum Cascade Lasers”. In: *physica status solidi (a)* 218.3 (2021), p. 2000407.

[64] Federico Capasso et al. “Quantum cascade lasers: ultrahigh-speed operation, optical wireless communication, narrow linewidth, and far-infrared emission”. In: *IEEE Journal of quantum electronics* 38.6 (2002), pp. 511–532.

[65] Haim Manor and Shlomi Arnon. “Performance of an optical wireless communication system as a function of wavelength”. In: *Applied optics* 42.21 (2003), pp. 4285–4294.

[66] Maha Achour. “Free-space optics wavelength selection: 10 μm versus shorter wavelengths”. In: *journal of optical networking* 2.6 (2003), pp. 127–143.

[67] CP Colvero, MCR Cordeiro, and Jean Pierre von der Weid. “FSO systems: Rain, drizzle, fog and haze attenuation at different optical windows propagation”. In: *2007 SBMO/IEEE MTT-S International Microwave and Optoelectronics Conference*. IEEE. 2007, pp. 563–568.

[68] Thomas Plank et al. “Wavelength-selection for high data rate Free Space Optics (FSO) in next generation wireless communications”. In: *2012 17th European Conference on Networks and Optical Communications*. IEEE. 2012, pp. 1–5.

[69] Jingye Sun, Fangjing Hu, and Stepan Lucyszyn. “Predicting atmospheric attenuation under pristine conditions between 0.1 and 100 THz”. In: *IEEE Access* 4 (2016), pp. 9377–9399.

[70] Laurence S Rothman et al. “The HITRAN2012 molecular spectroscopic database”. In: *Journal of Quantitative Spectroscopy and Radiative Transfer* 130 (2013), pp. 4–50.

[71] Alexander Berk et al. “MODTRAN4 radiative transfer modeling for atmospheric correction”. In: *Optical spectroscopic techniques and instrumentation for atmospheric and space research III*. Vol. 3756. International Society for Optics and Photonics. 1999, pp. 348–353.

[72] SA Clough et al. “Atmospheric radiative transfer modeling: A summary of the AER codes”. In: *Journal of Quantitative Spectroscopy and Radiative Transfer* 91.2 (2005), pp. 233–244.

[73] Alexander Berk et al. “MODTRAN® 6: A major upgrade of the MODTRAN® radiative transfer code”. In: *2014 6th Workshop on Hyperspectral Image and Signal Processing: Evolution in Remote Sensing (WHISPERS)*. IEEE. 2014, pp. 1–4.

[74] Jony J Liu et al. “Mid and long-wave infrared free-space optical communication”. In: *Laser communication and propagation through the atmosphere and oceans VIII*. Vol. 11133. International Society for Optics and Photonics. 2019, p. 1113302.

[75] Chloé Sauvage et al. “Study of short and mid-infrared telecom links performance for different climatic conditions”. In: *Environmental effects on light propagation and adaptive systems II*. Vol. 11153. International Society for Optics and Photonics. 2019, p. 111530I.

[76] Hamza Dely et al. “10 Gbit s- 1 Free Space Data Transmission at 9 μm Wavelength With Unipolar Quantum Optoelectronics”. In: *Laser & Photonics Reviews* (2021), p. 2100414.

[77] THIERRY Aellen et al. “Feasibility study of free-space quantum key distribution in the mid-infrared”. In: *Quantum Information and Computation* 8.1&2 (2008), pp. 0001–0011.

[78] Christian Weedbrook et al. “Quantum cryptography approaching the classical limit”. In: *Physical review letters* 105.11 (2010), p. 110501.

[79] Xiao Liu et al. "Practical aspects of terahertz wireless quantum key distribution in indoor environments". In: *Quantum Information Processing* 17.11 (2018), pp. 1–20.

[80] Carlo Ottaviani et al. "Terahertz quantum cryptography". In: *IEEE Journal on Selected Areas in Communications* 38.3 (2020), pp. 483–495.

[81] Lixing You. "Superconducting nanowire single-photon detectors for quantum information". In: *Nanophotonics* 9.9 (2020), pp. 2673–2692.

[82] Emma E Wollman et al. "Recent advances in superconducting nanowire single-photon detector technology for exoplanet transit spectroscopy in the mid-infrared". In: *Journal of Astronomical Telescopes, Instruments, and Systems* 7.1 (2021), p. 011004.

[83] Francesco Bellei et al. "Free-space-coupled superconducting nanowire single-photon detectors for infrared optical communications". In: *Optics express* 24.4 (2016), pp. 3248–3257.

[84] Alexander Berk, Patrick Conforti, and Fred Hawes. "An accelerated line-by-line option for MODTRAN combining on-the-fly generation of line center absorption within 0.1 cm-1 bins and pre-computed line tails". In: *Algorithms and Technologies for Multispectral, Hyperspectral, and Ultraspectral Imagery XXI*. Vol. 9472. International Society for Optics and Photonics. 2015, p. 947217.

[85] JM Martin and Stanley M Flatté. "Intensity images and statistics from numerical simulation of wave propagation in 3-D random media". In: *Applied Optics* 27.11 (1988), pp. 2111–2126.

[86] Jason Schmidt. "Numerical simulation of optical wave propagation with examples in MATLAB". In: Society of Photo-Optical Instrumentation Engineers. 2010.

[87] Rod Frehlich. "Simulation of laser propagation in a turbulent atmosphere". In: *Applied Optics* 39.3 (2000), pp. 393–397.

[88] Alexander A Kokhanovsky. *Aerosol optics: light absorption and scattering by particles in the atmosphere*. Springer Science & Business Media, 2008.

[89] Donald F Swinehart. "The beer-lambert law". In: *Journal of chemical education* 39.7 (1962), p. 333.

[90] Craig F Bohren and Donald R Huffman. *Absorption and scattering of light by small particles*. John Wiley & Sons, 2008.

[91] Orazio Svelto and David C Hanna. *Principles of lasers*. Vol. 4. Springer, 1998.

[92] Stefano Pirandola. "Satellite quantum communications: Fundamental bounds and practical security". In: *Physical Review Research* 3.2 (2021), p. 023130.

[93] Andrei Nikolaevich Kolmogorov. "The local structure of turbulence in incompressible viscous fluid for very large Reynolds numbers". In: *Proceedings of the Royal Society of London. Series A: Mathematical and Physical Sciences* 434.1890 (1991), pp. 9–13.

[94] Larry C Andrews and Ronald L Phillips. "Laser beam propagation through random media". In: SPIE. 2005.

[95] LC Andrews, RL Phillips, and PT Yu. "Optical scintillations and fade statistics for a satellite-communication system". In: *applied optics* 34.33 (1995), pp. 7742–7751.

[96] CE Coulman et al. "Outer scale of turbulence appropriate to modeling refractive-index structure profiles". In: *Applied Optics* 27.1 (1988), pp. 155–160.

[97] Sergei S Chesnokov et al. *Numerical/Optical Simulation of Laser Beam Propagation Through Atmospheric Turbulence.* Tech. rep. MOSCOW STATE UNIV (USSR), 1995.

[98] Mikhail Charnotskii. "Four methods for generation of turbulent phase screens: comparison". In: *arXiv preprint arXiv:1911.09185* (2019).

[99] Xuzhou Liu et al. "Numerical simulation of ground-to-satellite laser transmission based on unequal spacing phase screen". In: *2019 18th International Conference on Optical Communications and Networks (ICOCN)*. IEEE. 2019, pp. 1–3.

[100] Mark T Gruneisen et al. "Adaptive spatial filtering of daytime sky noise in a satellite quantum key distribution downlink receiver". In: *Optical Engineering* 55.2 (2016), p. 026104.

[101] Mark T Gruneisen, Michael B Flanagan, and Brett A Sickmiller. "Modeling satellite-Earth quantum channel downlinks with adaptive-optics coupling to single-mode fibers". In: *Optical Engineering* 56.12 (2017), p. 126111.

[102] Lijun Zhu et al. "Wave-front generation of Zernike polynomial modes with a micromachined membrane deformable mirror". In: *Applied optics* 38.28 (1999), pp. 6019–6026.

[103] Gianfranco Cariolaro. *Quantum communications*. Springer, 2015.

[104] Peter W Shor and John Preskill. "Simple proof of security of the BB84 quantum key distribution protocol". In: *Physical review letters* 85.2 (2000), p. 441.

[105] Xiongfeng Ma et al. "Practical decoy state for quantum key distribution". In: *Physical Review A* 72.1 (2005), p. 012326.

[106] Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen. "Decoy state quantum key distribution". In: *Physical review letters* 94.23 (2005), p. 230504.

[107] Miao Er-long et al. "Background noise of satellite-to-ground quantum key distribution". In: *New Journal of Physics* 7.1 (2005), p. 215.

[108] MT Gruneisen et al. "Modeling daytime sky access for a satellite quantum key distribution downlink mark". In: *Optical Society of America* 23 (2015).

[109] Dmytro Vasylyev, W Vogel, and Florian Moll. "Satellite-mediated quantum atmospheric links". In: *Physical Review A* 99.5 (2019), p. 053830.

[110] *WeatherSpark.com//Tucson.* `https://weatherspark.com/d/2857/6/21/Average-Weather-on-June-21-in-Tucson-Arizona-United-States#Figures-Temperature`.

[111] *WeatherSpark.com//Waterford.* `https://weatherspark.com/d/33020/12/21/Average-Weather-on-December-21-in-Waterford-Ireland#Figures-Temperature`.

[112] JM Gordon and M Hochman. "On the random nature of solar radiation". In: *Solar Energy* 32.3 (1984), pp. 337–342.

[113] Kyo Inoue, Edo Waks, and Yoshihisa Yamamoto. "Differential phase shift quantum key distribution". In: *Physical review letters* 89.3 (2002), p. 037902.

[114] RE Hufnagel and NR Stanley. "Modulation transfer function associated with image transmission through turbulent media". In: *JOSA* 54.1 (1964), pp. 52–61.