DIPLOMARBEIT

Simulating loss and solar photon noise in free-space satellite quantum key distribution during twilight stages

ausgeführt am Atominstitut
der Technischen Universität Wien

unter der Anleitung von
Univ.Prof Dr.rer.nat. Marcus Huber

durch

Katja Schneeweiss, BSc
Matrikelnummer: 11815160

October 23, 2024

Unterschrift StudentIn

I would like to express my gratitude to *qtlabs – Quantum Technology Laboratories GmbH* for enabling my thesis, with special thanks to Philipp Sohr and Manuel Erhard for their supervision. Thank you all for your support and mentorship.

Abstract

The importance of mitigating loss and noise in free-space satellite quantum key distribution (QKD) is significant. This thesis develops a model to simulate the impact of solar photon noise on the quantum transmission during twilight stages and their impact on achievable key rates. The model used to calculate twilight sky brightness is adapted from a previous approach, considering only single-scattering events and Rayleigh scattering. The number of photons for various angular positions of the sun is determined and utilized to calculate key generation rates for a decoy-state BB84 protocol. Combined with the simulations of beam spread loss for free-space QKD, estimations of maximum link distances for different twilight stages can be obtained. Many contributions to loss and noise were neglected, leading to an overestimation of the key generation rates and, thus, maximum link distances. The simulations, however, yield remarkably accurate results, considering the approximations and assumptions made. Therefore, the calculations provide a foundational basis for future model improvements, such as including additional loss mechanisms, atmospheric turbulence and multiple-scattering events.

Kurzfassung

Die Reduktion von Verlusten und Rauschen in der Freiraum-Satelliten Quantenschlüsselverteilung (Quantum Key Distribution, QKD) ist wesentlich. In dieser Arbeit wird ein Modell entwickelt, um den Einfluss von solaren Photonen und das von ihnen induzierte Rauschen auf die Quantentransmission während Dämmerungsphasen, zu simulieren. Das zur Berechnung der Helligkeit des Himmels in der Dämmerung verwendete Modell ist von einem früheren Ansatz abgeleitet und berücksichtigt nur Einzelstreuungsereignisse sowie Rayleigh-Streuung. Die Anzahl der Photonen für verschiedene Sonnenpositionen wird berechnet und verwendet, um die Schlüsselerzeugungsraten für ein Decoy-State BB84-Protokoll zu berechnen. Kombiniert mit der Simulation des Strahlverbreiterungsverlusts für Freiraum-QKD, können Schätzungen der maximal überwindbaren Transmissionsdistanzen für verschiedene Dämmerungsphasen berechnet werden. Viele Beiträge zu Verlusten und Rauschen wurden vernachlässigt, was zu einer Überschätzung der Schlüsselerzeugungsraten und somit der maximalen Transmissionsdistanzen führt. Die Simulationen liefern jedoch bemerkenswert genaue Ergebnisse, in Anbetracht der gemachten Annahmen und Vereinfachungen. Die Berechnungen bieten daher eine grundlegende Basis für zukünftige Modellverbesserungen, wie die Einbeziehung zusätzlicher Verlustmechanismen, atmosphärischer Turbulenzen und Mehrfachstreuungsereignissen.

Contents

1 Introduction and motivation

The encryption of secret messages has always been a race, ever since humankind invented methods to maintain some information secret. The various encryption schemes have advanced over the years and became more complex. Most of today's schemes are referred to as *computationally secure* because they rely on the assumption that the computational power required to break the encryption is not feasible with current technology.
However, this fundamental assumption cannot always be upheld [1]. Recent developments in building quantum computers pose a serious threat to those encryption methods, as they can utilize other algorithms, such as Shor's algorithm. As a result, quantum computers may be capable of decrypting currently used encryption schemes in the near future [2].

To prevent the secret data from being exposed, new cryptographic transmission methods have been developed. Post-quantum cryptography (PQC), for example, offers algorithms that aim to provide confidence even against quantum computers [3]. Nevertheless, these still rely on computational assumptions, meaning that once the encryption is broken, all messages can be deciphered subsequently.

To keep all information secret and to ensure that it cannot be deciphered retroactively, quantum key distribution (QKD) can be deployed. Unlike conventional encryption schemes, QKD exploits quantum mechanical principles to distribute a secret key for the encryption of messages. Since it no longer relies on computational complexity, it is regarded as *information-theoretically secure*, as arbitrarily large computational power cannot break the scheme [4]. QKD is often described as *unconditionally secure*, because, in theory, every eavesdropping attempt can be detected through error estimation [5]. This description, however, might be misleading as QKD does not rely on assumptions on the adversary's computational power, but does depend on assumptions about quantum mechanics [4].

Real implementations of QKD protocols induce various challenges in maintaining the secrecy of the key distribution [6]. For QKD channels can either use fiber or free-space transmission, most commonly with photons serving as qubits, to carry the transmitted information [4]. In both implementations, loss and noise within the channel are the main problems. A significant portion of transmitted photons is lost over long distances through either fiber or atmosphere, which reduces the length of the transmitted key [7]. Furthermore, noise within the channel leads to photons counts that were not generated by photons from the transmitter source. Those "wrong" counts induce errors, which cannot be distinguished from those induced by eavesdropping. Therefore, understanding and simulating noise induced by the environment is of utmost importance for developing and improving real QKD implementations [5].

1.1 Structure of the thesis

The aim of this thesis is to simulate some contributions to loss and noise for free-space satellite QKD during twilight stages and calculate key generation rates based on these findings.
In Section 2, we explain the fundamentals of quantum key distribution, its concept, advantages, assumptions and challenges. The subsequent section gives an overview of the practical implementations of QKD protocols in free-space, describing loss and noise contributions in the atmosphere, as well as a commonly utilized protocol.

In Section 4, the impact of beam spread on the quantum transmission is simulated, while Section 5 examines the impact of background noise, specifically solar photons reaching a receiver during different twilight stages. These found results are discussed in Section 6 and used in Section 7 to calculate key generation rates for different levels of background noise in a decoy BB84 protocol. Moreover, a preliminary comparison to experimental data is made to assess the accuracy of the simulations performed in this thesis.

For the Sections 1 to 3, ChatGPT was utilized to improve wording and phrasing. For Sections 4 to 8 and the Abstract, it was used to eliminate language and phrasing mistakes.

2 Theory of quantum key distribution

Quantum key distribution (QKD) utilizes quantum mechanical principles to encrypt information in qubits. The main advantages compared to classical encryption are that the encryption method is *information-theoretically secure* and, therefore, cannot be broken by even arbitrarily large computational power. Secondly, eavesdropping can (in theory) always be detected by error estimation, as this interference always causes an error [4]. However, real implementations of the QKD protocol face various problems and technical challenges [7].

To exploit quantum mechanical principles for distributing information, quantum bits known as qubits are employed. Most commonly, photons and their polarization degree of freedom are selected as qubits. Other degrees of freedom, such as orbital angular momentum, position-momentum, the number of sent photons and more can also be utilized. Quantum key distribution exploits the fact that measurements must be performed to obtain information about the observed system. Quantum mechanical measurements alter the observed states depending on the measurement basis.

In QKD, two non-orthogonal bases are randomly chosen for preparation and measurement of the qubits. Once the qubit transmission is completed, solely classical post-processing is performed. As part of this phase, sifting, parameter estimation, error correction, and privacy amplification are deployed. During this phase, the secure key is extracted from the received raw key [7].
The following section discusses the concept, assumptions, advantages, and most commonly deployed protocols.

2.1 From classical to quantum cryptography

Classical encryption algorithms can be categorized into two major classes. The *asymmetrical cryptosystems*, which use a public-key, allowing Alice and Bob[1] to utilize different keys for encryption and decryption. The most widely used algorithm, known as RSA, was first implemented in 1978 by Rivest, Shamir and Adleman. It relies solely on computational complexity, specifically the factorization of large integers. If the factors of the product are known, decoding the message is straightforward; whereas, if they are not, enormous computational power would be required to break the key [7, 8]. It is worth mentioning that the time required to decode the product grows exponentially with the number of bits in the code. Therefore, this scheme belongs to the *computationally secure* methods [4].

The second class is comprised of *symmetrical cryptosystems*, which utilize a secret key. In contrast to asymmetrical cryptosystems, Alice and Bob use the same key for encryption and decryption. Introduced in 1926, the *one-time pad* (OTP) is an example of this class. The concept is straightforward. Alice encrypts the message using a random secret key. She sends the resulting ciphertext to Bob using a public channel, which is not secure.[2] Afterwards, Bob receives the message and decrypts it using the same key. Eve could copy the ciphertext by listening to the channel, but has

[1] In cryptography, Alice and Bob commonly refer to the sending and receiving parties. Alice sends her encrypted message or a secret key to Bob, who deciphers it. An eavesdropper, trying to obtain knowledge about the key and the secret message, is usually called Eve [7].

[2] A *public channel* means that Eve can listen to and gather information transmitted through this channel but cannot interfere with or alter the message. A channel through which Eve could interfere is called an *insecure* channel [9][p.7]

no information about the secret key, leaving her with a random sequence of bits [7, 10].

The one-time pad, unlike the RSA scheme, is categorized as *information-theoretically secure*, conveying that arbitrarily high computational power cannot break the key [4]. "Actually, this is today the only provably secure cryptosystem!" [7]. Yet, this statement must not be misunderstood, given that many problems of implementation are excluded from this proof. Nonetheless, the one-time pad itself is provably secure. However, it has to meet the following three characteristics to be considered information-theoretically secure [4], as proven by Shannon in 1949 [11]:

- The key must be truly random, which is a challenging requirement to fulfill. Developing methods for generating such a key without any correlations between the bits is a current field of research.
- As the name of the method indicates, the key can only be used for encryption once and must be at least as long as the message.
- How to exchange a common secret key, without Eve gaining knowledge about it, has to be addressed separately. Either Alice and Bob meet in person to exchange keys securely, or they may use a trusted messenger, who is addressed as Charlie [4, 7].

Quantum key distribution is employed to address the last of these three challenges. It does not constitute a new class of encryption but enables communicating parties to exchange a secret key without sharing it with potential eavesdroppers.

To discuss the application of QKD, it is essential to first define what constitutes a key in the context of OTP. Alice aims to encrypt a secret message composed solely of 0s and 1s. Before sending it to Bob, she uses a key, as long as the message, containing a sequence of random bits (0s and 1s). Alice performs a bitwise addition (modulo 2)[3] of the key with her message, leaving her with a ciphertext that contains no information. Assuming Bob possesses the same key as Alice and the cipher was transmitted via a public channel, he again performs a bitwise addition (modulo 2) of the key and the ciphertext to decrypt it [9].

2.2 Fundamentals of quantum mechanics

To transmit a secret key, Alice and Bob exploit some fundamentals of quantum mechanics. In quantum mechanics, gathering information about a quantum state requires performing a measurement. Quantum mechanical measurements, however, perturb the initial state, resulting in its alteration for future measurements. First, we introduce two non-orthogonal bases $\{|0\rangle, |1\rangle\}$ and $\{|+\rangle, |-\rangle\}$, which can be expressed as superpositions of each other as

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \qquad \text{and} \qquad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \tag{2.1}$$

If the basis used to prepare the state is $\{|0\rangle, |1\rangle\}$ and the basis selected for measurement is $\{|+\rangle, |-\rangle\}$, the outcome will either be $|+\rangle$ or $|-\rangle$, corresponding to one of the basis states of the measuring basis. Therefore, without knowledge of the preparation basis, the measured states will inevitably

[3] Modulo 2 refers to the computational operation XOR (exclusive or), meaning $0 + 0 = 0$, $0 + 1 = 1$, $1 + 0 = 1$ and $1 + 1 = 0$ [9]

be altered [12].

Another fundamental principle is the no-cloning theorem. This states that one cannot copy a qubit (state) perfectly if it is not fully known and is a consequence of the *linearity of quantum theory* [9]. Therefore, it is not possible to copy a state, measure the copy, and leave the original state unaltered.

Additionally, the concept of "intrinsic randomness of quantum states and measurements" [4] is worth mentioning. This leads to the following effect: Assume a state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, with α, $\beta = [0,1]$ and $\alpha^2 + \beta^2 = 1$, but otherwise random α and β. If one measures said state, $|\psi\rangle$ in the basis $\{|0\rangle, |1\rangle\}$, the outcome will be $|0\rangle$ with probability $P_0 = \alpha^2$ and $|1\rangle$ with probability $P_1 = \beta^2$. In quantum mechanics, a combination of $|0\rangle$ and $|1\rangle$ cannot be measured [12].

With the aforementioned effects, it becomes possible to develop protocols that are, in theory, unbreakable and enable communicating parties to detect any eavesdropping attempt. In Section 2.3 the BB84 protocol, one of the most commonly deployed protocols is discussed in greater detail [6].

2.3 The concept of QKD protocols: The BB84 protocol

Discrete variable (DV) protocols can be divided into two classes. These classes include entanglement-based QKD protocols and *prepare & measure* protocols. The first QKD protocol, known as the BB84 protocol, was developed by Bennett and Brassard in 1984 [13] and is the most well-known prepare & measure protocol [6].

	Position of bit	1	2	3	4	5	6	7	8	9	10	11	12	13	14
(a)	Alice's random bits	1	1	0	0	0	0	1	0	1	0	0	1	1	1
(b)	random sending bases	D	R	R	R	D	R	D	D	D	R	D	R	R	D
(c)	sent photons	+	1	0	0	−	0	+	−	+	0	−	1	1	+
(d)	random measuring bases	D	D	R	R	R	R	D	D	R	D	D	R	D	D
(e)	Bobs measured bits	1	0	0	0	1	0	1	0	1	1	0	1	0	1
(f)	Bob reports bases	D	D	R	R	R	R	D	D	R	D	D	R	D	D
(g)	Alice confirms bases	✓		✓	✓		✓	✓	✓			✓	✓		✓
(h)	sifted key	1		0	0		0	1	0			0	1		1
(i)	Bob reveals some bits			0					0						
(j)	Alice confirms them			✓					✓						
(k)	Remaining shared Key	1			0		1	1				0	1		1

Table 2.1: Theoretical step-by-step description of the BB84 protocol, showing the quantum transmission, public comparison, key extraction and the error estimation process.

A simple overview of the steps of the BB84 protocol is presented in Table 2.1. Every QKD protocol can be divided into two parts. The first part is known as *quantum key transmission* (steps (a) to (e)), while the second part is referred to as *post-processing* (steps (f) to (k)), which is a purely classical process. Beginning with quantum key transmission, the first step (a) involves Alice having her random secret key, which consists of 0s and 1s. In the second step (b), Alice randomly selects the preparation basis for each qubit to be either the rectilinear (R) $\{|0\rangle, |1\rangle\}$, or the diagonal basis (D) $\{|+\rangle, |-\rangle\}$ [4]If at the corresponding position in her key is a 0, she chooses either $|0\rangle$ or $|-\rangle$ as her initial state [5], and sends the photon in the prepared state to Bob (step (c)). Bob, on the other hand,

[4]These are superpositions of each other as shown in Equation 2.1.
[5]For a 1 in the corresponding position, she selects $|1\rangle$ or $|+\rangle$, depending on the preparation basis.

also selects his measurement basis at random, similarly to Alice, to be either R or D, as shown in step (d). If Bob chooses the same basis for his measurement as Alice did for the preparation of that qubit, which occurs for 50 % of the sent photons, Bob obtains the correct state with certainty. If Bob does not select the same basis as Alice, his results will be completely uncorrelated, meaning his measured state will align with Alice's key bit with a probability of 50% and differ with a probability of 50%, regardless of the sent state. This leads to Bob's key, agreeing with Alice's key with a probability of 75%. These keys are referred to as the *raw key* (step (e)) [12].

Once the key transmission is completed, Alice and Bob use a public channel to compare their basis choices. A public channel allows Eve to listen to all communication occurring within this medium. In the next step (f), Bob reports the basis choices for all measured photons to Alice. Alice then confirms whether she chose the same basis for preparation or refutes it. Both parties abort all qubits and the corresponding bits for which they utilized different bases, as these yield uncorrelated results and therefore do not carry any information. Both parties retain only the bits for which their basis choices align, resulting in the *sifted key* (step (h)). For a perfect setup, both keys would be completely identical. It is evident that neither Alice nor Bob can influence the resulting key, as it is a random combination of the states of some of the sent qubits. Consequently, the key strings themselves do not convey any information.

To gain knowledge about the number of errors in their key, which is defined as the *quantum bit error rate (QBER)*, Alice and Bob perform the *parameter estimation*. In this step, they agree to announce a fraction of their sifted key publicly, compare those bits and estimate the QBER (step (i) to (j)). All announced bits are discarded from the key, as they are no longer secret (step (k)). To understand the reason for the parameter estimation, it is useful to explain a potential eavesdropping attempt on the BB84 protocol [4, 6, 12].

2.3.1 Eavesdropping attempts - The intercept-resend-attack

Eavesdropping mechanisms can be separated into three different types of attacks. The separation depends on the power that Eve is assumed to have. The *individual* attacks are the simplest, in terms of Eve's abilities, and are the ones most commonly discussed. The *intercept-resend attack* is part of this class. Security must also be provided against *collective* and *coherent* attacks, with the latter assuming that Eve has unlimited resources and is only restricted by the laws of quantum mechanics. Security proofs against these attacks are much more difficult to establish, however, also must be satisfied. In the following, for a better understanding, the simplest one, the intercept-resend attack, is discussed [12].

If we now assume that a third adversarial party attempts to gather information about the secret key, it would need to perform quantum measurements. Since all information about the secret key shared through the public channel is the basis choice after measuring, it does not contain any information about the resulting bit. When Eve, the adversary, knows the two non-orthogonal bases and the key bits they refer to, she can attempt to perform measurements on the sent photons as they travel from Alice to Bob and then send the measured photon further to Bob.

Eve has to choose her measurement basis at random, as Alice and Bob do. If Alice and Bob select different bases, the resulting key bits are discarded anyway, so Eve's interference would not

matter. However, if Alice and Bob choose the same basis and Eve performs a measurement on the sent photon, she has a 50% chance of guessing the correct basis for her measurement. If she does, she obtains the correct results and does not alter the qubit state. In this case, her interference cannot be detected. However, in 50% of the measurements of the sent photons, Eve does not guess the basis correctly. Let us assume Alice and Bob are using the rectilinear basis and Eve chooses the diagonal basis. In that case, Eve would observe the state to be $|+\rangle$ or $|-\rangle$ with equal probability of 50%. To avoid detection, she must send that photon to Bob, who then performs a measurement in the rectilinear basis. Regardless of whether the state that Eve sent is $|+\rangle$ or $|-\rangle$, he will measure the photon to be either $|0\rangle$ or $|1\rangle$, again with a probability of 50% for each.Assuming that Eve measures every sent photon, this leads to a disagreement of 25% in the keys held by Alice and Bob.

With this in mind, the communicating parties can identify Eve's interference by comparing a small part of their sifted key publicly, referred to as parameter estimation. If the QBER f is 0, they can be certain that Eve did not listen, meaning she did not perform quantum measurements on the sent photons, therefore does not possess any information about the shared key. However, if the error rate is $f = 25\%$, they abort the key and do not use it to encrypt a secret message, since Eve could have gathered information about it. [6]

In realistic implementations, a defined error threshold is established. If the QBER falls below this threshold, the key is utilized (after further post-processing steps). If it exceeds the threshold, the key is aborted and never used to encrypt secret information. If the protocol does not get aborted, further steps are executed. To reduce the errors in their key strings, Alice and Bob utilize a classical *error correction* protocol, which also reduces the key length. As Eve may have gained knowledge of some part of the key, the final step, called *privacy amplification*, is performed. This step also reduces the key length, while enhancing the privacy, thereby minimizing Eve's knowledge [4, 6, 12].

2.3.2 Concepts, advantages and assumptions of QKD

To employ QKD protocols of any kind, one needs two channels. A quantum channel is needed to distribute the qubits, and a public classical channel is required. The latter refers to a classical channel that a potential eavesdropper can listen to but cannot alter. This means the protocol functions if Eve knows which bases Alice and Bob chose for each photon, but she must not be able to modify the sent classical information.

Contrary to what the term *unconditionally secure* might suggest, QKD relies on certain assumptions. The key assumption in QKD is that quantum theory is correct. Due to this, it assumes that Eve can perform all kinds of quantum mechanical measurements within the quantum channel, but is restricted by the rules of quantum mechanics. However, no assumptions are made about Eve's computational power or technological abilities. For instance, this means that all observed errors have to be assumed to be induced by Eve, even if other sources of these errors are identified. The lack of assumptions about Eve's technological capabilities means that even quantum computers cannot compromise the key, as no amount of computational power can break it.

Another major advantage of QKD over computationally secure methods is that, in the latter, one cannot say with certainty whether an adversary has listened to the secret message. One can only

[6] Of course, Eve could measure only half of the sent photons, for example, leaving her with half the information about the key, resulting in an error rate of $f = 12.5\,\%$.

state that this is highly unlikely. For QKD protocols, however, one can find an eavesdropper by comparing parts of the sifted key. As explained earlier, if the QBER is too high and is assumed to be induced by Eve, the key gets aborted and is not used to encrypt information. This provides two advantages. First, one can be certain if anyone has gained knowledge of the key or message. Secondly, if she is able to obtain some information during the key transmission process, the communicating parties just discard the key and do not use it for anything. Thus, even if Eve intercepts, she gains no information about the secret message.

RSA schemes rely on the assumption that it would take too much time to crack the key, with today's achievable computational power. However, quantum computers are on the rise and could potentially increase achievable computational power by orders of magnitude, rendering currently employed methods insecure. Although such computers are not available today, they could threaten already encrypted and sent messages. Conventionally encrypted messages can be recorded and stored by a potential adversary. If quantum computers become available with the required computational power, these stored messages could subsequently be deciphered. This creates a new challenge regarding *long-term security*, which currently employed methods cannot guarantee [4, 6].

QKD schemes can be considered "*future-proof*" [4], as they cannot be broken by any computational power. Additionally, if the key is successfully distributed and the eavesdropper fails to intercept it during the process, that key cannot be broken subsequently, providing long-term security in contrast to computationally secure methods [4, 6].

2.4 Imperfections in the QKD channel

In Section 2.3 the theoretical concept of QKD was presented. However, when sending qubits through a quantum channel, perfect transmission is unattainable because a perfect quantum channel does not exist. Therefore, some of the sent photons get lost on their way to the receiver. In common implementations, a significant portion of the sent photons is lost. This loss is measured in decibels (dB) and severely impacts the obtained key rates.

Due to the no-cloning theorem, the signal cannot be amplified without inducing noise, meaning altering the initially sent states [4]. Loss and the resulting reduction of shared qubits between Alice and Bob directly impacts the length of the extractable key, as one cannot send an arbitrary number of photons per second (see Section 3.1.1). In realistic implementations, loss primarily affects the key length, which may become impractically small at some point, but would not influence the security, as shown by the figures in Section 7.

However, photon loss is not the only imperfection of the quantum channel. Not all bits that Bob receives lead to the correct outcome, even without Eve's interference, resulting in a non-zero QBER. As it signifies the rate of the erroneous bits relative to the total number of measurements, the QBER plays a significant role in the description of noise during quantum transmission [7, 12].

Noise refers to "wrong" results, specifically erroneous bits in the key induced by environmental interactions. "Here "environment" refers to everything outside the degree of freedom used for the

encoding" [7], which will be assumed to be the polarization of photons in this thesis. The interaction with this environment leads to decoherence, perturbing the quantum states, consequently changes the encrypted information. Mitigating the impact of these interactions on the channel is a fundamental challenge of QKD implementations, as *noise* plays a crucial role in the security of QKD [14].

In order to ensure that Eve did not listen during the quantum key transmission, Alice and Bob compare a small random sample of their sifted keys during the error estimation step. If the QBER exceeds the threshold, they abort the protocol, as Eve could have listened. However, in realistic implementations, noise can arise from various sources, such as photons emitted by the sun reaching the receiver. To uphold the promise of QKD, that no assumptions are made about the channel and Eve's capabilities, the worst-case scenario must be assumed, implying that all noise is presumed to be introduced by Eve's interference [4, 12].

Noise contributions, such as environmental photons and dark counts in the detector, lead to uncorrelated clicks in the detector, which, as two outcomes are possible, are correct by coincidence in 50% of the cases, therefore inducing a QBER of 50%. To ensure that the system's QBER is below a previously defined threshold, the signal-to-noise ratio has to be sufficiently high [15]. This must be achieved by reducing both the loss of the sent signal and the contributions of noise within the channel [7, 9].

3 Realistic implementations and challenges

To implement QKD channels, one can choose either fiber or free-space for quantum transmission. In this thesis, we will focus on free-space satellite QKD. Wireless optical communication is advantageous for long transmission channels compared to fiber, as the signal's attenuation scales quadratically, while it scales exponentially for fiber implementations [14, 16]. Both implementations offer advantages for different requirements. Free-space channels require a line of sight, while fiber implementations are more challenging to realize, since a fiber channel must be established and built between both parties. As mentioned earlier, long-distance implementations may lead to excessive loss, rendering key transmission infeasible.

For free-space QKD, most commonly the wavelengths $\lambda = 850\,\text{nm}$ and $1550\,\text{nm}$ are selected. At approximately 850 nm, there is a high transmission window that leads to reduced attenuation in the atmosphere, as the atmosphere is "weakly dispersive and essentially nonbirefringent at these wavelengths" [7]. The second most commonly used wavelength is $\lambda = 1550\,\text{nm}$, which aligns with the typically used wavelength for fiber-based communication [7].

However, these implementations face many challenges. Loss and noise in the channel lead to imperfect key transmission, which must be considered when performing security proofs for the utilized protocols [17, 18].

3.1 Free-space satellite QKD

In this thesis, the impact of loss and noise in free-space satellite quantum communication is investigated. In the following section, we discuss the components and setup of these free-space links.

Generally, the setup requires a photon source, a quantum channel, and a detector. The source and detector are explained in Section 3.1.1 [1]. In free-space QKD, the atmosphere serves as the quantum channel, distributing the key between a ground station and a satellite. To illustrate the experimental communication channel between a satellite and a ground station, we reference the work by Liao et al. [14]. This paper presents satellite-to-ground QKD, referred to as a downlink, using the low-earth-orbit (LEO) satellite *Micius*, with a wavelength of $\lambda = 850$,nm, photons and their polarization as qubits, and a decoy state BB84 protocol, which aligns with the choices made for the calculations in this thesis.

In said setup, a photon source suitable for LEO satellite operations is integrated into the satellite Micius, sending photons through the atmosphere to a fixed optical ground station (OGS) on earth's surface [14]. LEO satellites are typically found at altitudes of 2000 km and lower, but can be as low as 160 km [19]. Micius can be assumed to be 500 km above sea level. However, one of the downsides of satellite communication is that a constant link between transmitter and detector cannot be established. The overpass duration of a LEO satellite over an OGS is typically only about a few minutes per day. For Micius and the ground station based in Xinglong, China, the usable time for key extraction is 273 s per day. Furthermore, during these 273 s, the link distance, loss, angular position of the satellite, and extractable key rate vary significantly [14]. A usual satellite overpass over an OGS is illustrated in Figure 3.1. At this point it is worth noting that, in most cases, the satellite's path does not pass directly over the OGS. Instead, it maintains a

minimum distance defined by the minimum ground track distance between the OGS and the satellite, denoted as d_{min}. At this position, the maximum elevation angle θ_{max} is reached, as shown in Figure 3.1(a). For angles smaller than θ_{min} (as shown in Figure 3.1(b)), quantum transmission is no longer possible [20].

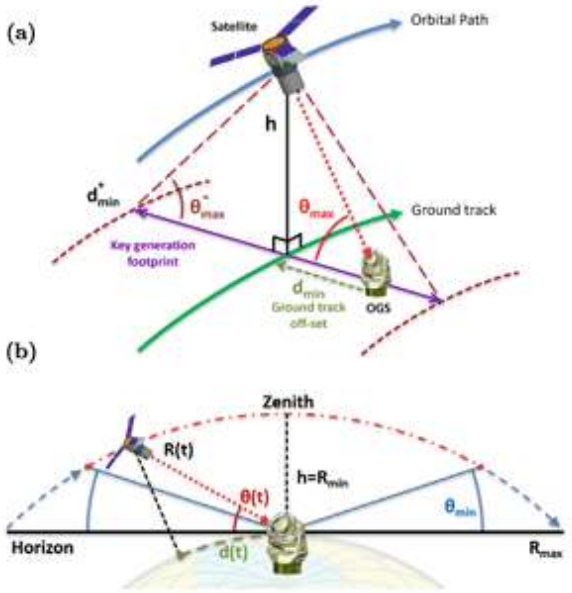

Figure 3.1: Geometric visualization of a LEO satellite overpass over a ground station. (a) d_{min} refers to the minimum ground distance between the satellite and the OGS for an overpass, at which the maximum elevation angle θ_{max} is reached (b) θ_{min} refers to the minimum angle of the satellite related to the zenith, at which quantum transmission is possible. Taken from [20].

In Figure 3.2 the link distance d in kilometers for different LEO satellites, in relation to the overpass time, is visualized. The significant variations in link distance during an overpass can easily be observed [21].

Liao et al. [14] utilized a downlink scenario, which demonstrates higher transmission efficiencies due to the reduced impact of beam wander (see Section 3.2.3). They employed a standard Cassegrain telescope, which was also assumed to be used in Section 4 for the loss simulations conducted in this thesis. Additionally, it is important to note that these experiments were limited to nighttime operations due to the significant impact of solar background noise during the daytime. The maximum link distance for quantum key distribution between the satellite Micius and the OGS in Xinglong was reported to be 1200 km. They found the signal loss to be approximately 22 dB, and the beam diameter to be about 12 m at that distance [14].

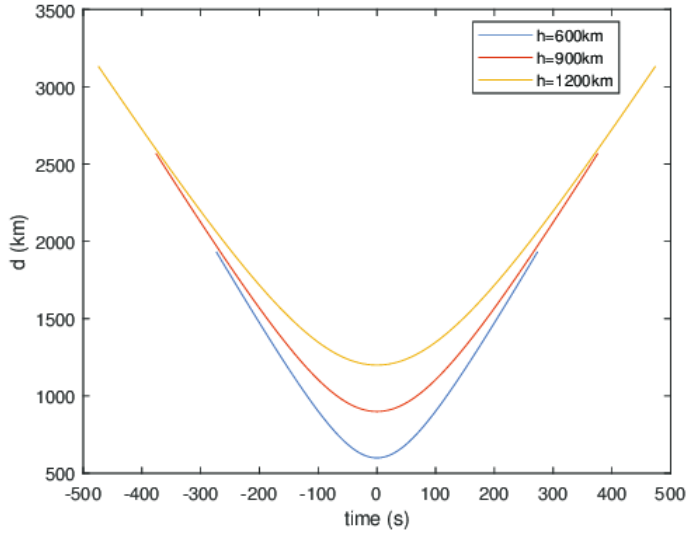

Figure 3.2: Distance between a LEO satellite to a receiver, related to the overpass time. $t = 0$ defined as the moment at which the minimum link distance occurs. The significant variations in the link distance during the quantum transmission process can be easily observed. Taken from [21].

3.1.1 Real implementations of photon sources and receivers

To achieve perfect QKD, single photons must be prepared and sent from Alice to Bob. However, true single photon sources do not exist, necessitating alternative implementations. Commonly, *weak coherent pulses* (WCP) are utilized as photon sources. These are lasers that emit, on average, significantly less than one photon per pulse [6]. The weak coherent pulse serves as an approximate single photon source, following the Poisson distribution. Alice sends a phase-randomized coherent state

$$\rho = e^{-\mu} \sum_{n=0}^{\infty} \frac{\mu^n}{n!} |n\rangle \langle n| , \tag{3.1}$$

where μ refers to the average photon number of the laser pulse, typically with values around $\mu \approx 0.1$.
Most of the time, the source does not emit any photons, resulting in a vacuum state with a probability $P(0) = e^{-\mu} \approx 90.5\%$. The probability of sending exactly one photon is $P(1) = \mu e^{-\mu} \approx 9\%$, known as single photon event. Multi-photon events, where more than one photon is emitted, occur with a probability of $P(n > 1) \approx 0.5\%$. Although these multi-photon events rarely occur, they entail risks of exploitation, as discussed in Section 3.3 [12, 22].

The photon detection after the transmission also brings along imperfections, as usually *threshold detectors* are deployed. These detectors measure whether at least one photon is present in the receiver. In other words, it cannot distinguish between a single photon and a multi-photon event. This indistinguishability introduces another vulnerability to the implementation. Furthermore, the detector efficiency is not perfect, leading to some single or multi-photon events not causing a click within the detector, while some vacuum events do cause a click. These false clicks, where no photon reaches the detector, are referred to as dark counts (DC) [6]. While improving photon detectors is an important area of research, it is not the focus of this thesis.

3.2 Sources of loss and noise in free-space QKD

In free-space satellite quantum key distribution, various environmental factors affect quantum transmission, causing both loss and noise in the channel. The following sections discuss some of the primary effects on the quantum transmission.

3.2.1 Geometric and misalignment losses

Considering the real implementation of free-space QKD, the decoy state BB84 protocol, presented in Section 3.3, utilizes a weak coherent laser pulse for photon transmission. These weak coherent laser pulses are modeled as a Gaussian beam, following [23]. An optical beam on its path through any medium, however, spreads along its way. In free-space optical communication, the narrow field of view leads to beam spread loss, as part of the beam escapes the detector, resulting in energy loss [23–25]. Said beam spread is analyzed in Section 4. A laser beam in the atmosphere additionally spreads due to diffraction of the beam.

Theoretically, narrowing the beam as much as possible would be advantageous. However, other imperfections must be considered. Pointing loss, caused by misalignment between the receiver and transmitter and imperfect tracking systems, can result in significant degradation of system performance. While increasing beam narrowing is beneficial in theory, a broader signal can mitigate the impact of misalignment-induced losses [24, 25].

3.2.2 Atmospheric absorption and scattering

Atmospheric loss occurs even under clear sky conditions. Part of the optical field's energy is transferred to molecular elements of the atmosphere, leading to a reduction in the optical signal along its path, a process known as absorption. The impact of said absorption heavily depends on the wavelength of the optical signal.

In addition to absorption, scattering effects also contribute to atmospheric loss. These scattering effects can be categorized into two types. The first is Rayleigh scattering, which involves scattering by atmospheric particles at the molecular scale, describing those with diameters much smaller than the signal wavelength. It strongly depends on the signal's wavelength, exhibiting a characteristic λ^{-4} dependence. The second is Mie scattering, which describes the interaction of light with atmospheric particles equal to or larger than the wavelength [26]. Therefore, Mie scattering models the interaction of light with particles such as dust, pollen, pollutants and aerosols, and is not strongly λ-dependent [26, 27]. Under clear-sky conditions, Rayleigh scattering dominates [26].

In Rayleigh scattering, the probability that a photon is scattered at a certain angle θ, relative to its original path, is described by the scattering phase function. Since it exhibits a $(1 + \cos^2\theta)$-dependency, one can conclude that the probability that the photon is not deviated is relatively high, as is the likelihood of backscattering at 180 degrees. The probability of being deflected by approximately $\theta = 90°$ is lower, as visualized in Figure 3.3 [28, 29].
Furthermore, it is necessary to point out that scattering effects not only impact the optical signal but also cause sky radiance, which induces noise [24], which is further investigated in Section 3.2.3. This effect is accounted for in this thesis to calculate noise contributions during twilight stages in Section 5.

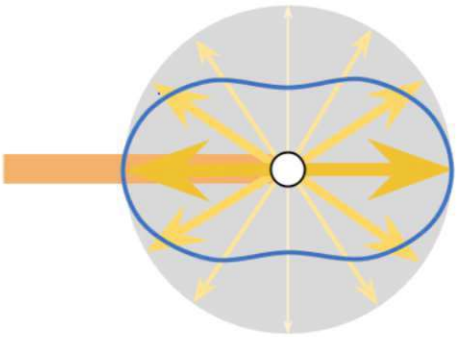

Figure 3.3: Schematic visualization of Rayleigh scattering. Taken from [28].

3.2.3 Atmospheric turbulence

Another critical factor to account for in free-space Sat-QKD is atmospheric turbulence. Characterizing said turbulence in the atmosphere is highly complex. Although the effects of turbulence are not included in the calculations in this thesis, they must be introduced due to their significant real-world impact.

To describe turbulence, the atmosphere is assumed to be a vicious fluid. Turbulent eddies are caused by inhomogeneities in atmospheric temperature and pressure, which result from wind and solar heating. These eddies vary in size and in turn affect the light beam in different ways. They cause random fluctuations in signal properties such as amplitude and phase, leading to a further reduction of the system performance.

Atmospheric turbulent eddies are typically characterized by three parameters. These parameters are the inner scale of the eddy l_0, the outer scale of the eddy L_0, and the refraction structure parameter C_n^2, also known as turbulence strength. A well-known theory for describing atmospheric turbulence is the *Kolmogorov theory* [24, 25].

In optical communication, turbulent eddies lead to additional effects depending on their size. *Beam wander* occurs when the eddies are larger than the size of the transmitter beam. Due to that, the beam is randomly deflected, altering its path. *Beam scintillation*, also known as fading, results in random focusing and de-focusing of the optical signal, much like an optical lens, causing random fluctuations in the signal's irradiance. If the eddies are smaller than the transmitter beam size, only a fraction of the beam is deflected independently of the rest of the beam, causing additional *beam spread* [24, 25].

It is worth mentioning that beam wander primarily affects uplink satellite communication and can be neglected for downlink implementations. This can be argued to occur due to the beam size in downlinks being much greater already, when the beam enters the atmosphere, making it larger than most of the eddies. However, in uplinks, the effects of beam wander must be taken into account [24].

3.2.4 Background radiation and noise

In addition to the effect on the optical signal itself, background radiation or ambient noise leads to an increase of noise in the channel since the receiver cannot distinguish between the signal and background radiation. The primary sources of this noise are direct, reflected, and scattered sunlight. Despite the existence of various technologies to mitigate its effects, ambient noise lowers the signal-to-noise ratio and, in some cases, even disables the quantum key transmission due to detector saturation [25]. These mitigation technologies include spatial filtering, spectrum filtering, temporal filtering, and the selection of a narrow bandwidth [14, 25, 30].

The electromagnetic radiation emitted by a source, in this case the sun, can be described using Planck's law of black body radiation

$$R(\lambda, T_{se}) = \frac{2hc^2}{\lambda^5} \frac{1}{\exp(hc/\lambda k T_{se}) - 1}. \tag{3.2}$$

Here, c denotes the speed of light, h is the Planck constant, k represents the Boltzmann constant, λ is the wavelength of interest, and T_{se} represents the temperature of the sun [26].

According to [30], the noise induced by solar photons differs significantly between day and night by as much as five orders of magnitude. Daylight free-space satellite QKD is currently being developed since successful key distribution could only be achieved during nighttime for a long time [30]. In order to enable daylight satellite QKD, understanding solar photons and their impact is of major interest. Modeling the behavior of solar photons and the noise they introduce can help in developing improved technology. As part of this thesis, said solar background noise will be simulated during twilight stages in Section 5.

3.2.5 Further atmospheric contributions

Several key effects on optical communication have already been covered. This presentation does not claim to be complete. Other environmental factors include varying weather conditions. Link performance is highly sensitive to weather conditions, which include fog, snow, or rain. The impact of these environmental effects is commonly assessed using atmospheric visibility [24].

3.3 Realistic implementation: The decoy-state BB84 protocol

Challenges in implementing secure QKD apply to all kinds of protocols. For better understanding, in this section, threats, solutions and cutting-edge technology will be explained on the basis of the BB84 protocol.

Section 3.1.1 has already covered several challenges related to real-world implementations. The so-called photon-number-splitting attack (PNS) exploits the fact that ideal single photon sources do not exist, leading to the use of weak coherent pulses instead. The attack works as follows: Eve can perform a non-demolition measurement by measuring how many photons were sent, without disturbing the quantum state. If multiple photons were sent in that pulse, Eve stores one photon for herself and leaves the remaining ones to pass through to Bob. Since all photons in the same pulse are identically prepared, she now possesses a photon identical to the one Bob will measure. Eve then stores her photon and waits for Alice and Bob to compare their preparation

and measurement bases. Once Eve knows which bases they used, she can measure her photon in the same basis, gaining complete information about the key bit encoded in it.

If Eve detects that exactly one photon is sent, she can either let it pass through to Bob without gaining any information about its outcome. Alternatively, she can intercept or measure the photon herself, but since it won't be used by Alice and Bob for key extraction, this effectively results in photon loss [12, 22]. As most of the sent photons are naturally lost during transmission in free-space QKD, Alice and Bob cannot determine whether Eve is responsible for the loss of certain photons.

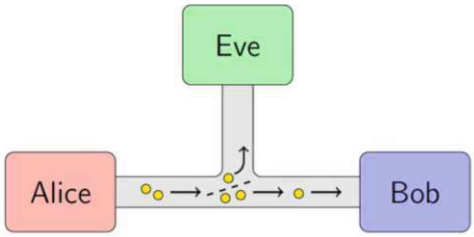

Figure 3.4: Schematic concept of the photon-number-splitting attack, with the yellow dots representing the sent photons. Taken from [12].

To mitigate the risk of a photon-number-splitting attack, countermeasures can be employed. The typically deployed scheme is the decoy-state protocol. For this strategy,, a second (sometimes even a third) weak laser pulse source is used. The so-called decoy source is identical to the signal source in every aspect except for the average photon number μ. In the decoy state, μ_{Decoy} is much larger (typically around 0.8) compared to the signal state, where $\mu_{Signal} = 0.1$. Now, Alice randomly sends either a signal state or a decoy state. Bob continues to measure the incoming photons as usual. Eve cannot determine whether the sent state is a signal or a decoy state, forcing her to perform the same measurements on all of the pulses. If Eve, using the PNS attack, stores a single photon from each pulse, her interference can now be detected by Alice and Bob. Once the key transmission is complete, Alice and Bob not only compare their chosen bases but also disclose whether the sent was a signal or a decoy state. The decoy states are not utilized to generate a shared secret key, instead, Alice and Bob compare the number of signals sent to the number of signals received.

The channel's transmittance should be consistent across all signals, meaning the same percentage of sent signals must successfully pass through the channel. However, if Eve stores one photon from each pulse, she alters the signal's transmittance differently based on different average photon numbers μ. By comparing the transmittance of the signal and decoy states, they can detect a photon-number-splitting attack and abort the protocol.

To avoid detection, Eve would have to refrain from interfering with most pulses, limiting her knowledge to only a small portion of the key, which could then be reduced even further by applying privacy amplification [12].

4 Simulating loss due to beam spread in satellite QKD

Beam spread is a major contribution to loss in free-space QKD. In the following, said loss will be calculated. Ideally, single photons are sent through the atmosphere, but to describe the spatial intensity distribution transverse to the propagation path, beam optics can be utilized.

4.1 The Gaussian beam and its beam spread

As light is electromagnetic radiation, it is expressed as a transverse electromagnetic wave (TEM), described by the wave equation

$$\nabla^2 u = \frac{1}{c^2}\frac{\partial^2 u}{\partial t^2}. \tag{4.1}$$

The derivation in this chapter follows that by Andrews et al. [23]. With the *complex amplitude* of the wave $U_0(R)$ and the field $u(R,t)$, one finds the Helmholtz equation

$$\nabla^2 U_0 + k^2 U_0 = 0. \tag{4.2}$$

For further calculations - as the wave is symmetric around the z-axis - cylindrical coordinates were chosen, leading to the form of the wave equation as

$$\frac{1}{r}\frac{\partial}{\partial r}\Big(r\frac{\partial U_0}{\partial r}\Big) + \frac{\partial^2 U_0}{\partial z^2} + k^2 U_0 = 0. \tag{4.3}$$

z refers to the propagation distance, as the beam is assumed to originate at the source and propagate along the positive z-axis, while r describes the distance to the z-axis along the propagation path.

Furthermore, one has to introduce the "paraxial approximation", which is discussed in further details in Appendix A.1. It assumes that the longitudinal propagation distance is much larger than transverse distance. With this approximation and $U_0(r,z) = V(r,z)e^{ikz}$ one finds the *paraxial wave equation* to be

$$\frac{1}{r}\frac{\partial}{\partial r}\Big(r\frac{\partial V}{\partial r}\Big) + 2ik\frac{\partial V}{\partial z} = 0. \tag{4.4}$$

For a further description of the propagating laser beam the *lowest order Gaussian-beam wave* (TEM_{00}[7]) is utilized, which can be assumed for the purposes of this thesis.
Since a collimated beam is assumed, $F_0 \to \infty$ must be fulfilled, which is numerically done by assuming that $F_0 = 10^{11}$ m.

[7] The index refers to the order of the mode, in this case 00, meaning the lowest order.

Name	description
F_0	Focal length - for collimated beam $\rightarrow \infty$
z	propagation distance - with source in $z = 0$
r	distance from the optical axis (z-axis)
a_0	amplitude of the beam at $r,\ z = 0$
W_0	effective beam radius (spot size)
k	wave vector

Table 4.1: Required input parameters for the Gaussian wave equation and their description

The lowest-order Gaussian beam wave at $z = 0$ is given by

$$U_0(r,0) = a_0 \exp\Big(-\frac{r^2}{W_0^2} - \frac{ikr^2}{2F_0}\Big) = a_0 \exp\Big(-\frac{1}{2}\alpha_0 kr^2\Big), \tag{4.5}$$

where W_0 refers to the spot size, which is the distance from the optical axis at which the value of the amplitude has dropped to $1/e$ of the initial value at the optical axis. Thus, it serves as a measure of the width of the Gaussian beam [23]. For free-space QKD applications, the beam width at the sending aperture W_0, can be selected as 8 cm [24].
The amplitude of the Gaussian beam for $z = 0$ is defined as

$$A_0 = a_0 \exp\Big(-\frac{r^2}{W_0^2}\Big), \tag{4.6}$$

and its phase ϕ_0 and α_0 can be found with

$$\phi_0 = -\frac{kr^2}{2F_0} \qquad \text{and} \qquad \alpha_0 = \frac{2}{kW_0^2}. + i\frac{1}{F_0} \qquad [m^{-1}]. \tag{4.7}$$

To find the solution, the direct solution ansatz

$$V(r,z) = A(z) \exp\Big[-\frac{1}{p(z)}\Big(\frac{\alpha_0 kr^2}{2}\Big)\Big] \tag{4.8}$$

is chosen.
With this in mind , along with further calculations, one finds the complex amplitude at distance z to be

$$U_0(r,z) = V(r,z)e^{ikz} = \frac{1}{1+i\alpha_0 z} \exp\Big[ikz - \frac{1}{2}\Big(\frac{\alpha_0 k}{1+i\alpha_0 z}\Big)r^2\Big] \tag{4.9}$$

$$= \frac{1}{1+i\alpha_0 z} \exp\Big[ikz - \frac{ik}{2z}\Big(\frac{\alpha_0 kz}{1+i\alpha_0 z}\Big)r^2\Big]. \tag{4.10}$$

To better handle of this equation, one introduces the new parameters

$$\Theta_0 = 1 - \frac{z}{F_0}, \qquad \Lambda_0 = \frac{2z}{kW_0^2}, \tag{4.11}$$

$$\phi = \tan^{-1}\frac{\Lambda_0}{\Theta_0}, \qquad \phi = \tan^{-1}\frac{\Lambda_0}{\Theta_0} \qquad \text{and} \qquad F = \frac{kW_0^2}{2}\Big[\frac{\Lambda_0(\Theta_0^2+\Lambda_0^2)}{\Theta_0(1-\Theta_0)-\Lambda_0^2}\Big], \tag{4.12}$$

which leads to

$$U_0(r,z) = \frac{1}{1+i\alpha_0 z}\exp\left[ikz + \frac{ik}{2z}\left(\frac{i\alpha_0 k}{1+i\alpha_0 z}\right)r^2\right] \tag{4.13}$$

$$= \frac{1}{\sqrt{\Theta_0^2+\Lambda_0^2}}\exp\left(-\frac{r^2}{W^2}\right)\exp\left[i\left(kz-\phi-\frac{kr^2}{2F}\right)r^2\right]. \tag{4.14}$$

After $U_0(r,z)$ is determined, one needs to find the intensity of the beam [23]

$$I^0(r,z) = |U_0(r,z)|^2 = \frac{1}{\Theta_0^2+\Lambda_0^2}\exp\left(-\frac{2r^2}{W^2}\right) \quad \text{in } [W/m^2]. \tag{4.15}$$

To demonstrate the beam spread as calculated above, the spot size of the beam $W(z)$ is showcased in Figure 4.1. At $z = 0$, referring to the origin of the laser beam, the spot size $W(z=0) = W_0$ is chosen to be 8 cm. One can observe that $W(z)$ to increases linearly with the distance z [23].

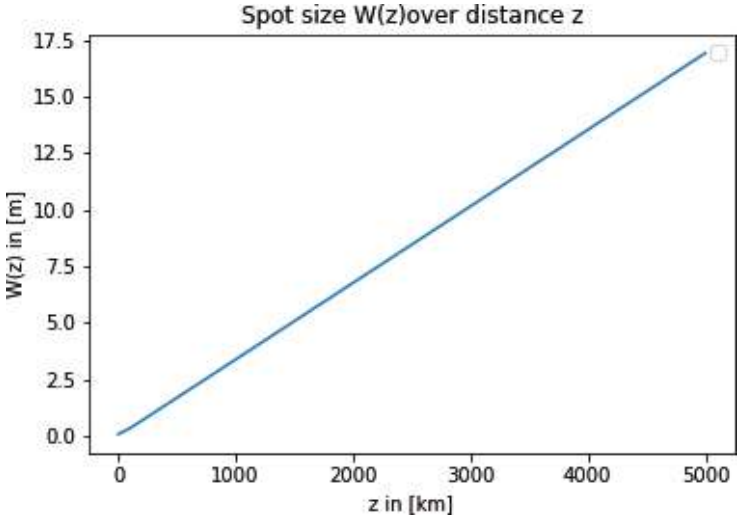

Figure 4.1: Increase of spot size $W(z)$, showing its linear increase related to the propagation distance z.

For the calculations in the following section, it is necessary to introduce the total power P at a distance z_0 from the receiver. This is accomplished by integrating over the entire plane orthogonal to the z-axis as

$$P_\infty = \int_0^{2\pi}\int_0^{\infty} |U_0(r,z)|^2 \, dr \, d\phi \tag{4.16}$$

$$= 2\pi\frac{1}{\Theta_0^2+\Lambda_0^2}\int_0^{\infty}\exp(-\frac{2r^2}{W^2})\,dr \tag{4.17}$$

$$= \frac{1}{2}\pi W_0^2, \tag{4.18}$$

which aligns with the calculation in [23]. Since no loss of power is assumed, the total power remains constant for all distances z [23].

4.2 Calculating the geometric efficiency η_{geom}

In this section, the previously discussed calculation by Andrews et al. [23] will be utilized as a basis to calculate the beam spread loss in terms of the geometric efficiency.

In QKD, light is utilized to transmit photons from a source to a receiver. This is often realized with a weak coherent pulse (WCP), which is deployed for decoy state protocols. The receiver, in a certain distance z_0 from the source, has a finite diameter. The radius of the receiver can be set to $r = 0.5$m [31]. If the propagation distance is large, as is commonly the case in free-space QKD, the beam spread prevents the entire beam from entering the receiver. The aim of this chapter is to calculate the part of the beam, which reaches the receiver, depending on z_0.

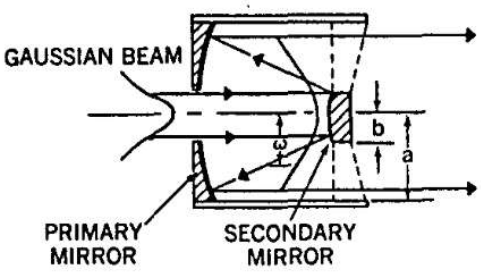

Fig. 1. Cassegrainian telescope.

Figure 4.2: Cassegrainian telescope set-up, including primary and secondary mirror. a refers to the radius of the primary mirror and b is the radius of the secondary mirror, with the latter obscuring the center of the telescope. Taken from [32].

For the geometric efficiency, one needs to find the fraction of the power P, that enters the receiver. To do this, one performs the same calculation as in Equation (4.16), but with different integration limits. Instead of integrating dr from 0 to ∞, as done in [23], one would integrate from 0 to $r_a = 0.5\,\text{m}$, which represents the radius of the receiver aperture. For more realistic calculations, however, at this point it is useful to take into account the geometrical structure of a commonly utilized telescope, as showcased in Figure 4.2. One finds the secondary mirror to be in the center of the z-axis, obscuring some part of the receiver. Therefore, the *obscuration ratio* γ is introduced. It is defined as the ratio of the circular secondary mirror's radius r_{min} and the telescope's radius r_a [32]. For deployed telescopes in free-space QKD links, one can assume the obscuration ratio to be $\gamma = r_{min}/r_a \approx 50\,\%$, leading to $r_{min} = 0.25\,\text{m}$ with $r_a = 0.5\,\text{m}$ [31]. This results in new integration limits for the power $P(z, r_a)$ reaching the receiver:

$$P_{receiver}(z, r_a) = \int_0^{2\pi} \int_{r_{min}}^{r_a} |U_0(r, z)|^2 \; dr \; d\phi \tag{4.19}$$

$$= \frac{\pi W_0^2}{2} \Big(\exp\left(-\frac{2\, r_{min}^2}{W(z)^2}\right) - \exp\left(-\frac{2\, r_a^2}{W(z)^2}\right) \Big). \tag{4.20}$$

As $W(z)$ increases with z, it is obvious, that $P(z, r_a)$ decreases with increasing propagation distance. Now, one can calculate the geometric efficiency $\eta_{geom}(z, r_a)$, which is defined as the ratio of the two found powers

$$\eta_{geom}(z, r_a) = \frac{P_{receicer}(z, r_a)}{P}. \tag{4.21}$$

Said geometric efficiency $\eta_{geom}(z, r_a)$ over the distance z is visualized in Figure 4.3.

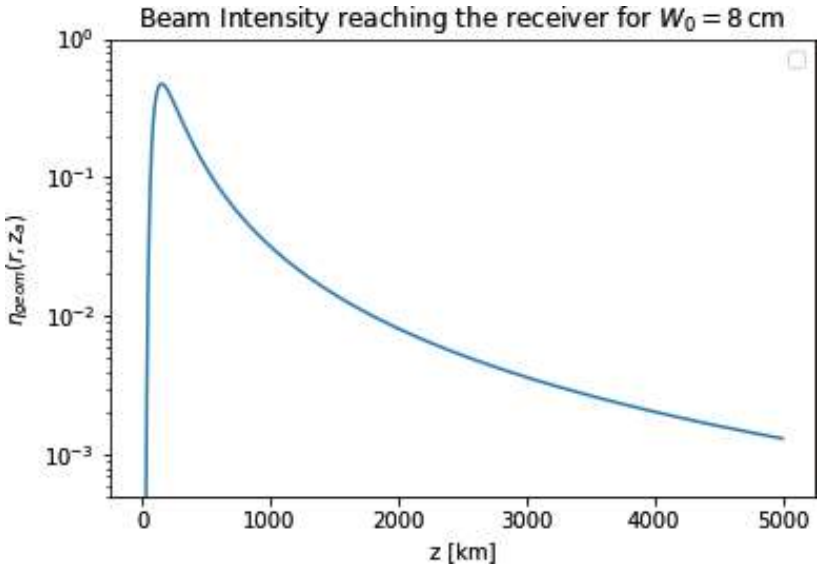

Figure 4.3: Geometric efficiency $\eta_{geom}(z, r_a)$ presented on a logarithmic scale describing the beam spread loss in free-space satellite QKD in relation to the link distance z, with an obscuration ratio $\gamma = 0.5$ and a beam sport size of $W_0 = 8$ cm at the source.

As expected, $\eta_{geom}(r, z_a)$ decreases significantly with increasing link distances. Due to the substantial reduction in geometric efficiency, the results are presented on a logarithmic scale to better capture and visualize the magnitude of this decline. The rapid increase observed at $z = 0$ originates from the area at the center of the receiver, which is obscured by the telescope. This is expected, as the beam is fully focused at the source with a beam width of $W(z = 0) = 8$ cm.

Unlike the noise simulation in Section 5, the calculated beam spread loss is valid for both uplinks and downlinks, since the beam spread depends on the propagation distance only. As discussed in Section 3.1 the link distance for an overpass of a usual LEO satellite varies from approximately 600 km up to 3000 km (Figure 3.2) [21]. To gain a better picture of the overall behavior of the loss in free-space QKD, the observed range was selected to be $z = [0\,\text{km},\ 5000\,\text{km}]$.

These results are combined with the noise simulations in Section 7.4, to estimate the key generation rate for a BB84 decoy state protocol.

5 Simulating noise in Sat-QKD during twilight stages

As the goal of this thesis is to investigate the impact of noise on a free-space satellite QKD link, this section examines the brightness during different twilight stages. The number of solar photons per second that reach receiver is calculated for a downlink scenario. These results will later be utilized to simulate possible key generation rates for different twilight stages in Section 7.

5.1 Models, literature and assumptions

This thesis builds upon "UBVRI twilight sky brightness at ESO-Paranal" by Patat et al. (2006) [29]. This paper aims to provide measurements and models to describe twilight sky brightness. It utilizes the UBVRI method, which employs passbands in the range of 366 to 798 nm. The paper investigates the sun zenith distance angles in a range of $94^o - 112^o$. As showcased in Figure 5.4, the angles are defined as the degrees to the horizon of the sun, relative to a point on the earth's surface.

Since the paper considers single-scattering events only in the atmosphere and neglects multiple-scattering events, it is a rather simple model, and can be reconstructed in this thesis. However, it must be noted that, by neglecting multiple-scattering, the model underestimates the brightness compared to the experimentally obtained data.

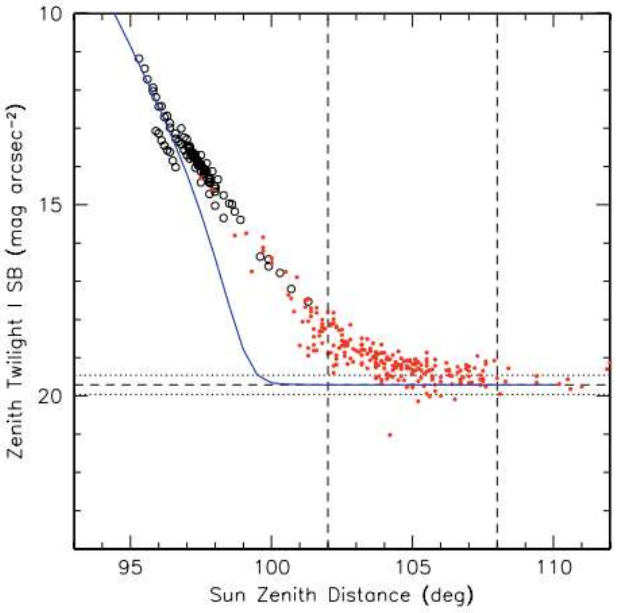

Figure 5.1: Modeled twilight sky brightness compared with experimental data from ESO-Paranal for the I passband (corresponding to $\lambda = 798$ nm) for positions of the sun, just below the horizon (90°), showing the decrease of brightness until it reaches the night sky brightness. Taken from [29].

5.1.1 Assumptions for the model

In order to calculate the twilight sky brightness, several assumptions where made for the model:

1. The earth is a sphere with radius $R_0 = 6380\,\text{km}$
2. The atmosphere extends to $\Delta R = 400\,\text{km}$
3. Numerical density of the atmosphere n(h) [8] is assumed according to the MSIS-E-90 model, that can be found in [33, 34].
4. There is no atmospheric refraction.
5. The Sun is treated as a point source, and all incoming rays are considered parallel.
6. Only single-scattering events are considered (multiple-scattering is neglected).
7. Only Rayleigh scattering is assumed to contribute to scattering (Mie scattering is neglected).

According to Patat et al. [29], the first five assumptions are valid and can be applied for these calculations. However, it is also noted that the last two assumptions lead to some deviations in the results in certain cases. Nevertheless, the results found by utilizing these models, approximately agree with the experimentally found data.

As stated in [35], multiple-scattering events can no longer be neglected at angular zenith distances over 96°, which corresponds to the beginning of nautical twilight. This is in good agreement with Figure 5.1, where the deviation of the experimental data and the predicted values can be observed. To get a better understanding of the expected behavior of the surface brightness curve, in Figure 5.3 the experimentally obtained sky brightness in lux for different angular positions of the sun related to the horizon is shown. It will be taken into account in the following sections to compare the found model, to experimental values [35].

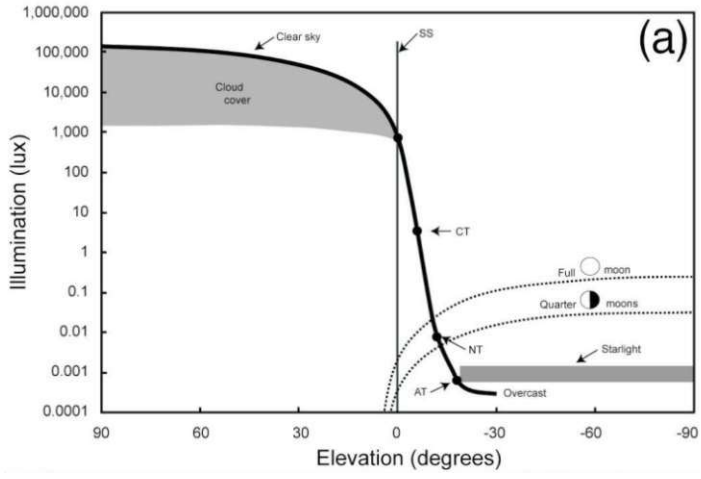

Figure 5.3: Experimentally obtained brightness for different angles of the sun relative to the horizon, showing the decrease during different twilight stages until it reaches night sky brightness. Taken from [35].

[8] Patat et al. [29] refer to the density as n, whereas in this work it is described as ρ.

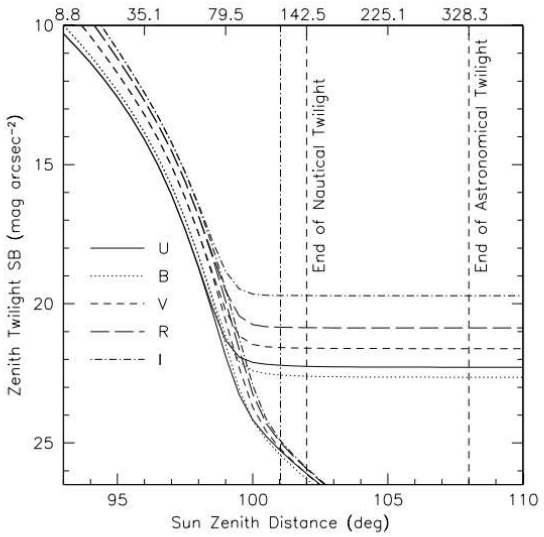

Fig. 1. Model twilight sky brightness at zenith. The thick curves include the night sky contribution, while the thin lines indicate only the scattered component. The vertical dashed-dotted line marks the Sun zenith distance when the lower boundary layer height is 120 km. The upper scale indicates the lower Earth's boundary layer height in km.

Figure 5.2: Modeled twilight sky brightness for different passbands at zenith (corresponding to $\alpha = 0°$). One can observe the impact of the added night sky brightness, as without it the brightness would continue to decrease. Taken from [29].

5.1.2 Twilight classification

When the Sun is at an angular zenith distance of $\phi < 90°$ relative to the receiver station, it is considered daytime. If this angle is $\phi > 108°$, it is classified as nighttime, during which the sky brightness remains approximately constant. The sky brightness decreases rapidly in the range of $90° < \phi < 108°$, which can be divided into three stages of twilight. The range from $\phi = 90°$ to $96°$ is termed *civil twilight*. *Nautical twilight* refers to the angles from $96°$ to $102°$, while *astronomical twilight* corresponds to angles between $\phi = 102°$ and $108°$. It is worth mentioning these definitions, as they are commonly used in literature and will be referenced throughout this work [35].

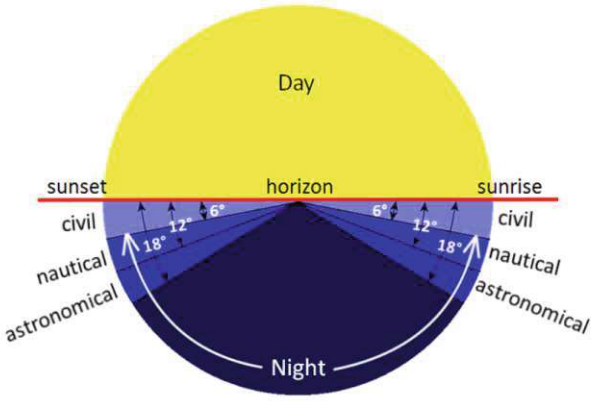

Figure 5.4: Stages of twilight: Between day and night, the three presented stages of twilight can be found, defined by the position of the sun below the horizon. Taken from [36].

5.1.3 Astronomy and utilized units

In astronomy, specific units are utilized. his section provides a brief explanation of the main units for better understanding and comparison of the figures.
Fixed wavelengths and bandwidths, referred to as passbands, are typically used when measuring brightness. Patat et al. [29] used the UBVRI passbands. In this thesis the focus is on the I-passband, as its wavelength of λ = 798nm is the one closest to 850 nm. Its effective bandwidth is $\Delta\lambda_{eff}$ = 0.15 μm = 150 nm. In astronomy the commonly utilized unit for the wavelength is μm, also called microns [37].

Brightness is measured in magnitudes, a dimensionless unit, that scales exponentially with the number of photons. It is defined over so-called zeropoints M_0, which are (arbitrarily) set values for different passbands. The brightness decreases with an increasing number of photons within the beam, allowing for negative values for very bright light [38]. Appendix A.6 presents the zeropoints, sun's magnitude, as well as the experimentally determined night sky brightness for the UBVRI passbands [39, 40]. These experimentally found zeropoints and the definition of the brightness make it impossible to recalculate the brightness for arbitrarily selected wavelengths. Therefore, the aim to recalculate the brightness for λ = 850 nm, cannot be reached as initially aimed.

5.2 Noise calculations

The aim of this thesis is to model the environmental photons emitted by the sun that reach the receiver. Therefore, it is necessary to calculate the attenuation and scattering of sun rays within the atmosphere. To find the results in photons per second, the total surface brightness must be calculated. The following sections present all required parameters and input values, either taken from Patat et al. [29] or calculated and adapted in this thesis.

5.2.1 Geometrical calculations

To determine the brightness at the receiver during twilight, specifically the sunlight scattered in the atmosphere that reaches the receiver, we first need to explain and calculate the geometry of

the setup. It is based on Figure A.1 from [29], which has been modified and is presented below as Figure 5.5. This chapter follows the calculations of Patat et al. [29] and outlines the necessary steps for this work. Table 5.1 provides an overview off all utilized values and parameters.

To determine the brightness of sunlight scattering into the receiver, it is necessary to find the transmittance of the sun's rays through the atmosphere. This transmittance depends on the density of scattering particles along the path of the beam. Since the density of scattering particles in the atmosphere is not constant and decreases with height above sea level (asl), it is necessary to determine the height above sea level (asl) for every point along the beam's path, depending on the angle of the field of view (FOV) α and the sun's angular position ϕ.

Name	Type	description
R_0	distance	earth radius (6380km)
ΔR	distance	assumed height of the atmosphere(400km)
α	angle	angle of the FOV in elation to the zenith/z-axis
ϕ	angle	angle distance of the sun's position related to the horizon
h_s	distance	height asl of the receivers position (small values necessary)
Q	point	Point, where sun ray enters atmosphere
H	point	point on path through atmosphere with minimum height als
P	point	point, where beam meets FOV/scatters in receiver
O	point	point of receiver
δ	distance	minimum height asl of beam / height als at point H. Minimum value is 0
l	distance	distance, which the scattered beam has to pass in the FOV from P to the receiver O
l_0	distance	minimum value of l, meaning distance from P_0 to O
l_1	distance	maximum value of l
h_0	distance	height asl of the point P_0
Q_0	point	Q at lowest possible beam path (where $\delta = 0$)
P_0	point	P at lowest possible beam path (where $\delta = 0$)
H_0	point	H at lowest possible beam path (where $\delta = 0$)
q	distance	describes the position on the beam's path through atmosphere. It ranges from $q = 0$ (at Q) to $q = QP$ (at P)
QH	distance	distance between the points Q and H
HP	distance	distance between the points H and P
QP	distance	distance between the points Q and P, is the sum of QH and HP
H_0P_0	distance	distance between the points H_0 and P_0
H_{QP}	distance	height asl at every point (dependent on q) on the beam's path
θ_R	angle	scattering angle on the FOV, that scatters into the receiver

Table 5.1: Overview over all values, parameters, points, distances and angles, that are visualized in Figure 5.5.

In Appendix A.2, detailed calculations and assumptions are explained similar to those in [29]. Using these, one can derive an expression for the height asl at every point along the atmospheric path $h_{QP}(\alpha, \phi, q, l)$, denoted as:

$$h_{QP} = \sqrt{(QH - q)^2 + (R_0 + \delta)^2} - R_0. \tag{5.1}$$

It requires α and ϕ as inputs, along with the position along the path q, and l, which means a specific height asl for the beam must be defined. These parameters contribute to Equation (5.1), as δ and the distance QH depend on α, ϕ, and l.

It is important to note that these calculations are valid, but are restricted by an upper bound for $|\alpha|$. $|\alpha|$ must be less than a maximum value which depends on ϕ. Furthermore, the calculations are performed for $\phi \geq 2°$, as for smaller values of ϕ, the calculations may diverge. The maximum value α_{max}, for which reliable results can be found, is approximately 20° for $\phi = 2°$, increasing to about $|\alpha_{max}| = 70°$ at $\phi = 10°$. The calculations, therefore, can be reliably used in ranges $\alpha = [-20°, 20°]$ and $\phi = [2°, 18°]$.

Calculations for higher angles $|\alpha|$ remain to be completes and are briefly discussed in Appendix A.2. However, we have calculated the geometry to also be valid for negative values of α.

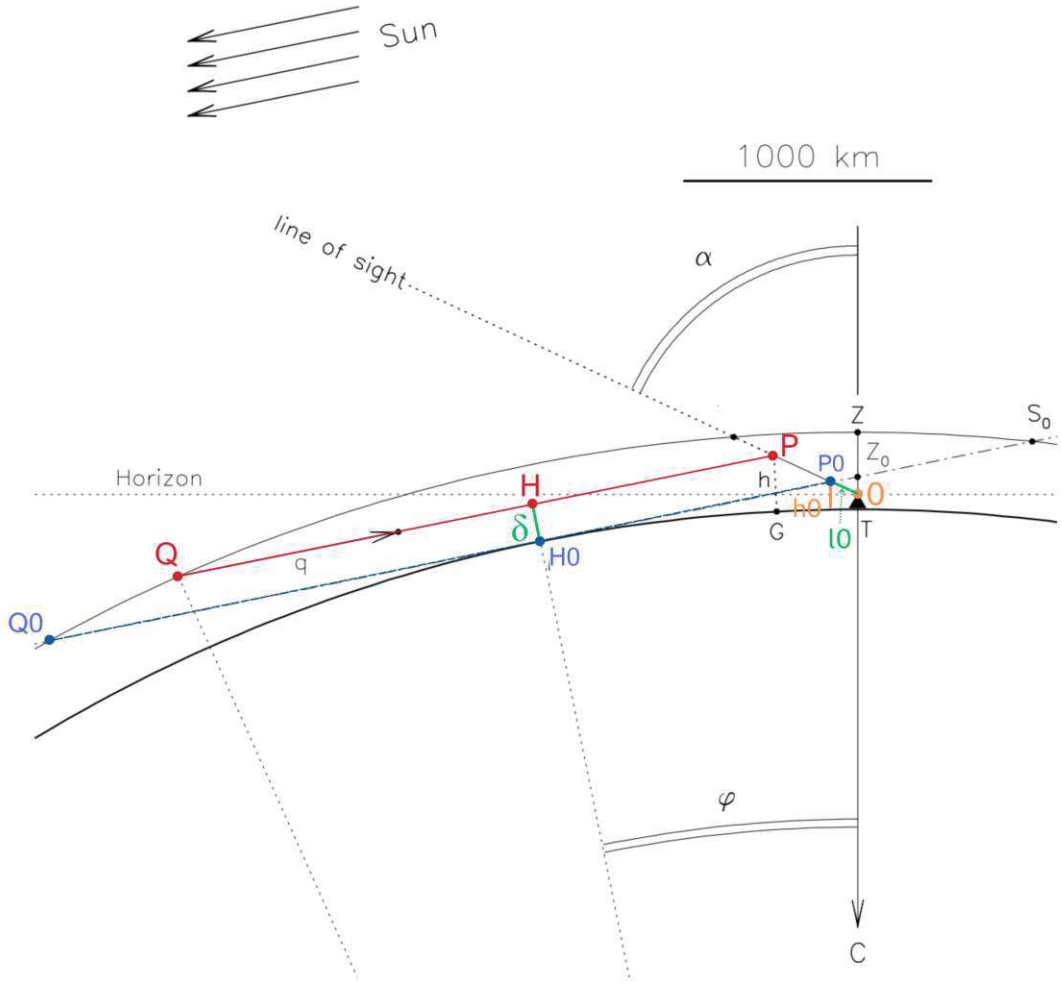

Figure 5.5: Geometrical considerations adapted and adjusted from Figure A.1 of [29].
With the receiver at O at height h_s asl, and the FOV rotated at angle α related to the zenith, the figure illustrates the path of the incoming sun ray for a fixed angular distance ϕ of the sun beneath the horizon. The beam enters the atmosphere at point Q and travels along q (the red line) to the point P in the FOV, where it is scattered into the receiver at O. The length from P to the receiver is referred to as l. Depending on ϕ and α, the height at which the beam crosses the atmosphere can vary. Point H is where the beam reaches its minimum altitude while traversing the atmosphere. This minimum altitude is denoted as δ and can vary from 0 to a certain maximum value. Q_0, H_0 and P_0 represent the positions of Q, H and P along the beams path at lowest possible height ($\delta = 0$). The distance from P_0 to O is referred to as l_0, while l_1 describes the longest possible path through the FOV. Thus, l_0 and l_1 denote the minimum and maximum values of l. Adapted from [29].

Some further parameters nee to be defined to obtain reasonable results for the calculations. As discussed in Section 3, the wavelengths of interest are $\lambda = 850\,\text{nm}$ and $\lambda = 1550\,\text{nm}$, as these two wavelengths are commonly utilized for free-space quantum key distribution and therefore of high interest for this study. For this work, $\lambda = 850\,\text{nm}$ was chosen.

The height above sea level of the receiver at O was arbitrarily set to $h_s = 800\,\text{m}$ for all plots showcased in this work.

5.2.2 The extinction cross section $C_{ext}(\lambda)$

To calculate the extinction cross section theoretically, it is assumed to equal the Rayleigh scattering cross section $\sigma(\lambda)$ [9]. The absorption coefficient is neglected here [23]. As discussed by A. Buchholtz in 1995 [41], the total Rayleigh scattering cross section is given in cm^2 as

$$\sigma(\lambda) = \frac{24\pi^3}{\lambda^4 N_s^2} \cdot \left(\frac{n_s^2 - 1}{n_s^2 + 2}\right)^2 \cdot F_k(\lambda). \tag{5.2}$$

The variable λ is contained with a λ^{-4}-dependency, which is characteristic of Rayleigh scattering and is also given in cm. N_s is the molecular number density, which is $N_s = 2.54743 \cdot 10^{19}\,\text{cm}^{-3}$ for standard air. n_s describes the refractive index of the air and is λ-dependent. Bucholtz [41] presented an equation for wavelengths greater than 230 nm, called the "four-parameter formula":

$$(n_s - 1) \cdot 10^8 = \frac{5791817}{238.0185 - \lambda^{-2}} + \frac{167909}{57.362 - \lambda^{-2}}. \tag{5.3}$$

For $\lambda = 850\,\text{nm}$, this yields $n_s = 1.00027$. Note that Equation (5.3) takes the wavelength as input in μm. The last factor $F_k(\lambda)$ is called the King correction factor, and yields from the depolarization, with ρ_n referring to the depolarization factor, as follows:

$$F_k(\lambda) = \frac{6 + 3\rho_n}{6 - 7\rho_n}. \tag{5.4}$$

The λ-dependency arises from the fact that ρ_n is λ-dependent. In [41], one can also find a table for the values of ρ_n, dependent on the wavelength. As no equations are presented to calculate ρ_n, this value must be taken as an input for the utilized λ values. For standard air and $\lambda = 850\,\text{nm}$, one finds $\rho_n = 0.0273$. Since $F_k(\lambda) \approx 1$, it does not have a severe impact and is not of greater interest for this work. Due to this, it will not be investigated further and is assumed to be a input parameter. After that, one can calculate the extinction cross section $\sigma(\lambda = 850\,\text{nm})$ and finds that $\sigma(\lambda = 850\,\text{nm}) = 7.7004 \cdot 10^{-28}\,\text{cm}^2$, which aligns with the values presented in [41].

Further investigation of the Rayleigh scattering cross section can be found in [42–45].

Calculation from the extinction coefficient $\kappa(\lambda)$

To confirm the above found results, another method to calculate the extinction cross section is utilized. As Patat et al. suggested in [29], one can find the extinction cross section $C_{ext}(\lambda)$ by utilizing the measured extinction coefficient $\kappa(\lambda)$. With $\tau_z(\lambda) = 1.086\,\kappa(\lambda)$, one can use

$$\tau_z(\lambda) = \rho_0 \cdot C_{ext}(\lambda) \int_{h_s}^{\Delta R} \frac{\rho(h)}{\rho_0}\, dh \tag{5.5}$$

[9] This can be done at least for N_2 in the atmosphere, which is the main component of the earth's atmosphere.

to find $C_{ext}(\lambda)$. To find reasonable values for κ, a previous publication by Patat et al. [46] from 2003 was taken into account. One can find $\kappa(\lambda = 800\,\text{nm})$ to be approximately 0.0025 magnitudes per air mass [mag/airmass][10]. Mag/airmass is a dimensionless unit that describes the loss of brightness per air mass. Air mass is a measure for the amount of air along the beam's path through the atmosphere. It scales with the altitude angle, starting with 1 air mass at the zenith, 2 air masses at 30° and increasing up to approximately 38 air masses at the horizon.
With these values, one can find $C_{ext}(\lambda = 800\,\text{nm}) = 7.996 \cdot 10^{-32}\,\text{m}^2$, with an assumed height asl of the ground station of $h_s = 800\,\text{m}$. ρ_0 and $\rho(\lambda)$ refer to the scattering particle density of the atmosphere, which is further described in Section 5.2.3 [29]. The two found values for the extinction cross section are approximately the same and therefore can be assumed to be correct [39].

5.2.3 Atmospheric scattering particle density $\rho(h)$

The scattering particle density $\rho(h)$ is given as the number of scattering particles per unit volume element [m^{-3}]. The density distribution of the scattering particles ρ is required as an input parameter for the calculation of the brightness from the sun that reaches the receiver. $\rho(h)$ depends on the height asl h and can be modeled with different assumptions.

Patat et al. [29] use the MSIS-E-90 Model presented by Hedin in 1991 [34], which is displayed in Figure 5.6 (solid line). It can approximately be described by the power law, for altitudes greater than 120 km. For altitudes of 120 km or lower, it can be assumed to follow an exponential curve [29].

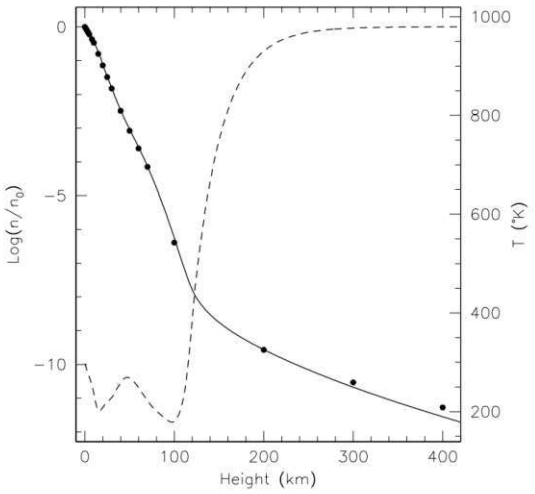

Fig. A.2. Normalized density (solid line) and temperature (dashed line) profiles according to the MSIS-E-90 model (Hedin 1991). For comparison, the dots trace the values of the US Standard Atmosphere (McCartney 1976, Table 2.6).

Figure 5.6: Experimentally found, normalized scattering particle density of the atmosphere by Hedin in 1991 [33]. Taken from [29].

For the calculations in this thesis, however, the distribution was assumed to follow a single

[10] Note that the ranges of wavelengths that were plotted only extend to 800 nm, but here $\kappa(\lambda = 800\,\text{nm}) = \kappa(\lambda = 850\,\text{nm})$ is assumed.

exponential function, which reads

$$\rho(h) = \rho_0 \cdot \exp(-a \cdot h). \tag{5.6}$$

Here, ρ_0 refers to the number of scattering particles per m^3 above sea level, which equals $N_s = 2.54743 \cdot 10^{25}\,m^{-3}$, as utilized for the cross section calculations in Section 5.2.2. The constant a was found by fitting to be $a = 0.7555 \cdot 10^{-4}$. It was calculated by investigating Figure 5.6, where one can find, that the density, dependent on height asl, drops about 12 orders of magnitudes over ΔR compared to ρ_0 [29]. Hence, the chosen value for a provides the most realistic density distribution. The visualization of the density distribution, along the path of the sun ray, utilized in the calculations can be found in Appendix A.2.2.

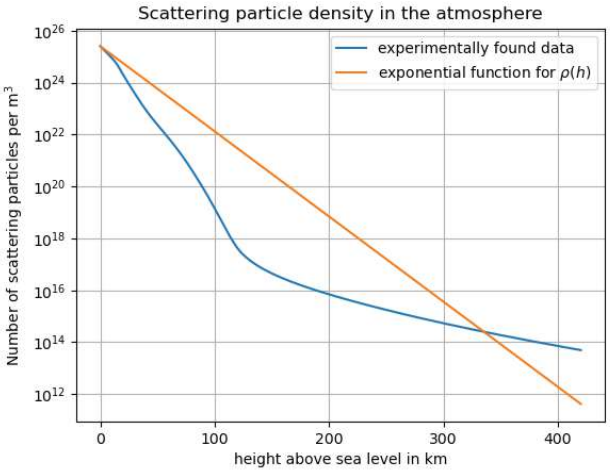

Figure 5.7: Experimentally found atmospheric scattering particle density [29, 34] (blue line) relative to the height above sea level h, scaled by the assumed fixed value for ρ_0, compared to the exponential density distribution chosen for the calculations in this thesis (orange line).

5.2.4 The scattering phase function $\Phi(\theta)$

In order to calculate the brightness, it is essential to introduce the scattering phase function $\Phi(\theta)$. As a parallel beam scatters at one fixed point, the scattering phase function describes the fraction, or the intensity, of light scattered at an angle θ. As presented in [29], the normalization condition for $\Phi(\theta)$

$$\int_{4\pi} \Phi(\theta)\, d\Omega = 1 \tag{5.7}$$

must be satisfied. Due to said normalization condition, the unit of the scattering phase function $\Phi(\theta)$ is $\left[\frac{1}{\text{sr}}\right]$. Steradians (sr) is a unit of solid angle, with 4π sr describing the entire surface of the sphere.
Patat et al. utilized Equation (5.7), which is based on the canonical expression for air molecules [47], combined with Equation (5.8), which reads

$$\Phi(\theta) = 0.0607\left[1 + 0.9324\,\cos^2(\theta)\right]. \tag{5.8}$$

This expression will also be utilized for the calculations in this thesis. Its distribution is visualized in Figure 5.8 [29, 40].

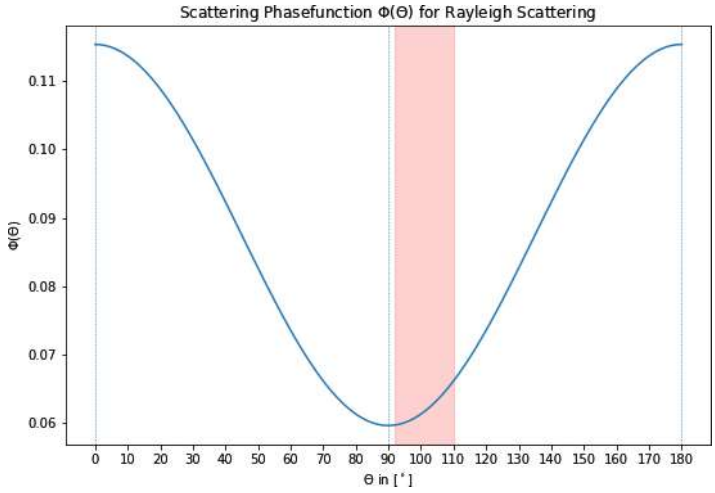

Figure 5.8: Scattering phase function $\Phi(\theta)$, based on [29]. The red area highlights the range of angles θ, that are relevant for scattering from the line of sight into the receiver.

By calculating values for θ relevant to the brightness calculations, one finds that for $\alpha = 0°$, θ ranges between 92° to 110° for $\alpha = 0°$, corresponding to the red area in Figure 5.8.
Comparing the observed behavior of the graph in Figure 5.8 and the visualization of Rayleigh scattering in Figure 3.3, one finds that these two figures consistent with one another.

5.2.5 Luminosity of the sun L_0

The sun's Luminosity L_0 is a fundamental input parameter for the calculation of the total brightness reaching the receiver. It is defined as the number of photons emitted per second per wavelength. The required factor F_0 for the brightness is related to the luminosity by

$$F_0 = \frac{L_0}{4\pi d^2}, \tag{5.9}$$

where d is the distance between the sun and the earth, meaning 1 astronomical unit (1AU) [29]. Attempting to calculate F_0 from the black-body radiation of the sun, did not yield reasonable results (see appendix A.3). Consequently, the calculation of F_0 was performed, using the same methodology as Patat et al. [29], following consultation with the author [40]. The reference values for the magnitude scale, commonly utilized in astronomy, were also used to find F_0. It is important to note that these reference values only exist for specific passbands (the UBVRI passbands), therefore the reference value for the I passband was used, since this is the one closest to $\lambda = 850$nm. F_0 is calculated as:

$$F_0 = 10\hat{}(-0.4\,(M_{sun} - M_0)), \tag{5.10}$$

where M_0 represents the photometric zero-point for the I passband, given as $M_0 = -12.70$ in [erg s^{-1} cm^{-2} μm^{-1}]. The sun's brightness for the passband of interest is $M_{sun} = -27.55$ mag (see Appendix A.6). Utilizing Equation (5.10) one finds that $F_0 = 8.709 \cdot 10^5$ erg/(cm^2 s μm), with 1 erg = 100 nJ (nanojoule). The unit [cm^{-2}] describes the area that is reached by the beam and μm

in the denominator represents the bandwidth of the observed wavelength λ [29].

For further brightness calculations, said value for F_0 is utilized. However, for comparison with later noise results, it is useful to convert this to number of photons per second per cm^2 per nm. This conversion is performed as described in Section 5.2.7. For the I passband, the number of photons emitted by the sun per second and nm is found to be $F_0(I) = 3.726 \cdot 10^{14}$ (s cm^2 nm)$^{-1}$ [29].

5.2.6 Optical depth τ

The optical depth τ is another essential physical quantity that must be introduced. It is important to note that this quantity is not derived in the same way as in [29]. The optical depth is a dimensionless ratio of incoming light compared to the transmitted light through a medium, in this case the atmosphere. We use the general definition of τ, given by

$$\tau(z) = \int_z^\infty n(z)\, \sigma_a\, dz \tag{5.11}$$

and can be found in [48]. It describes the integral over a path through a medium. In Equation (5.11), this path dz is vertical and extends from z (a specific height asl) to infinity. Here, $n(z)$ represents the density distribution, which will be referred to as $\rho(h)$ from now on. σ_a represents the cross section, corresponding to $C_{ext}(\lambda)$, which was already introduced earlier in Section 5.2.2. The optical depth τ is related to the transmittance by the expression

$$T = e^{-\tau} \tag{5.12}$$

This relationship is dimensionless and lies within the range [0,1] [48].
In this work, it is necessary to calculate τ along its path through the atmosphere, which is not vertical. Therefore, some modifications have to be made:
To find the total optical depth τ_Σ, one needs to integrate over the path dq or dl, starting from point Q, following along q, passing through H and reaching point P. From there on, the path continues along l to the receiver at O. It is useful to divide τ_Σ in sections and sum them afterwards. First, one calculates τ_{QH}, meaning the optical depth along the path from Q to H. The second section covers the path from H to P, represented by τ_{HP}, followed by the path within the FOV, described by τ_{OP}. This leads to the following equations:

$$\tau_{QH}(l) = C_{ext}(\lambda) \int_H^Q \rho(h_{QP}(l,q))\, dq, \tag{5.13}$$

$$\tau_{HP}(l) = C_{ext}(\lambda) \int_P^H \rho(h_{QP}(l,q))\, dq \quad \text{and} \tag{5.14}$$

$$\tau_{OP}(l) = C_{ext}(\lambda) \int_O^P \rho(h_{QP}(l,q))\, dl. \tag{5.15}$$

Some important points should be highlighted regarding Equations (5.13) - (5.15):

- Implicit dependencies on the angles α and ϕ are not explicitly states, as the brightness calculations are performed for fixed values of these angles.
- dq and dl represent the infinitesimal paths through the atmosphere, corresponding to the sun ray's path, defined as q and l in Section 5.2.1.

- Since the extinction cross section $C_{ext}(\lambda)$ is assumed to be independent of the altitude, it can be factored outside of the integral.
- All calculations for τ are made for one specific path, meaning it requires a fixed value for l as input. This dependency is shown by writing $\tau(l)$.
- The density ρ depends on the altitude h_{QP}, which in turn depends on l. As defined in Equation (5.1), h_{QP} is written here as $\rho(h_{QP}(l))$.
- In this thesis, the results are obtained through numerical integration.
- The total optical depth $\tau_\Sigma(l)$ is computed as the sum of the optical depths for the three segments as $\tau_\Sigma = \tau_{QH} + \tau_{HP} + \tau_{OP}$.

5.2.7 Calculating the total brightness

The primary goal of this thesis is to develop a model to describe the amount of noise present in the channel during the distribution of polarized photons. The main contribution to noise in QKD during twilight are unpolarized photons emitted by the sun. In order to characterize this noise during twilight, one has to determine the so-called brightness at the receiver. Brightness is measured in mag/arcsec^2, representing magnitude per arcsecond (MPSAS). It is a logarithmic unit representing brightness per unit of solid angle. One arcsecond equals 1/3600 degrees or approximately 4.848 μrad and 1 sr = $4.26 \cdot 10^{10}$arcsec^2, as already discussed in Section 5.1.3.

The detailed derivation of Equation (5.26) is provided in Appendix A.4 and follows the calculations by Patat et al. [29]. It is derived from df, which represents the number of photons received per unit time, area, and wavelength.
By differentiating df with respect to $d\Omega$, which represents the solid angle, one obtains the surface brightness db, describing the brightness emitted from an infinitesimal small volume [11] To calculate the total brightness b that scatters into the receiver, an integration is performed over all possible paths, resulting in the integration limits l_0 and l_1, as they represent the minimum and maximum height asl of the incoming beam.

$$b = F_0\, C_{ext}(\lambda)\, \Phi(\theta) \int_{l_0}^{l_1} \rho(h(l))\, e^{-\tau_\Sigma(l)}\, dl \tag{5.16}$$

yields the total surface brightness scattering into the receiver, as presented by Patat et al. [29]. With reasonable input values, it will be possible to calculate the number of photons from the brightness [49].
It is worth noting, that the unit of b is [erg / (s cm^2 μm sr)], with sr referring to steradians or square radians, which is the unit for the solid angle. To convert this result to arcseconds squared, one has to divide the initial result by $4.26 \cdot 10^{10}$ [40].

Surface brightness: Unit conversions

Having found the total brightness reaching the receiver in [erg / (s cm^2 μm arcsec^2)], it must be converted to [mag / arcsec^2], in order to compare with the results from Patat et al. [29], using

$$B[\text{mag/arcsec}^2] = -2.5\, \log_{10}(\, b[\text{erg}/(\text{s cm}^2\, \mu\text{m arcsec}^2)] \,+\, b_{night}\,) \,+\, M_0. \tag{5.17}$$

[11] The volume depends on the height of the path, which is a function of l.

b_{night} refers to the night sky brightness, which is an experimentally found value, that has to be added, to get comparable results. It is defined as

$$b_{night} = 10\hat{}(\,0.4\,(M_0 - M_{night})), \tag{5.18}$$

with $M_{night} = 19.7$.
In order to do so, one has to assume that the values for the I-passband ($\lambda = 798\,\text{nm}$) also apply for $\lambda = 850\,\text{nm}$, as was already done for F_0 [50, 51].

5.2.8 Calculating the number of photons reaching the receiver

For the calculation of noise in the channel, however, the results must be found in photons per second. Therefore, the following adjustments were made as part of this thesis. To convert the brightness from energy to the number of photons [(s cm^2 nm arcsec^2)$^{-1}$], the following equation is used:

$$b[(\text{s cm}^2\,\text{nm arcsec}^2)^{-1}] = \frac{10^{-7}\cdot 10^{-3}}{E_{photon}(\lambda)} \cdot b[\text{erg} / (\text{s cm}^2\,\mu\text{m arcsec}^2)], \tag{5.19}$$

with

$$E_{photon}(\lambda) = \frac{hc}{\lambda} \tag{5.20}$$

describing the energy of a photon at wavelength λ. In order to later calculate the resulting noise, the number of photons reaching the receiver must be determined in [s^{-1}], requiring the removal of the units [cm^2 nm arcsec^2].
To achieve this, further assumptions are necessary. One should note that the following assumptions are made to approximate the achievable key generation rates in Section 7,and are thus approximations, not exact calculations.
First, the angle α is fixed at $\alpha = 0$ for the following calculations, to simplify understanding. The geometrical visualization of the following calculations is shown in Figure 5.9.
The calculations in previous chapters account for the scattering phase function $\Phi(\theta)$, which introduces the unit [sr^{-1}]. To eliminate the dependency on the solid angle, $\Phi(\theta)$ from Equation (5.8) must be integrated over all angles that reach the receiver, as [12]

$$\int \Phi(\theta)\,d\Omega = \int \Phi(\theta)\,\sin(\theta)\,d\theta\,d\phi = \Delta\phi \int \Phi(\theta)\,\sin(\theta) d\theta \tag{5.21}$$

$$= \Delta\phi \cdot 0.0607\Big[\cos\theta + 0.9324 \cdot \frac{1}{3}\cos^3\theta\Big]\Big|_{\theta-\Delta\theta}^{\theta+\Delta\theta}. \tag{5.22}$$

Since $\Phi(\theta)$ is independent of the angle ϕ,it appears only occurs as a multiplication factor in the equations. Next, one needs to determine the integration limits for the angle θ. The opening angle $\Delta\theta$ must be calculated for each scattering point during the integration over dl from l_0 to l_1 in Equation (5.26), as it depends on the distance from the scattering point to the receiver. As a first approximation, we assume that a fixed opening angle $\Delta\theta$ can be calculated for a specific angular position ϕ of the sun. To achieve this, we calculate the average l_{middle} of the minimum l_0 and maximum value l_1 for the given angle ϕ, and use it to compute the opening angle

$$\Delta\theta = \tan(\frac{r_a}{l_{middle}}) = \tan(\frac{2\,r_a}{l_0 + l_1}). \tag{5.23}$$

[12] This is valid due to the normalization of the scattering phase function $\int_{4\pi} \Phi(\theta)\,d\Omega = 1$.

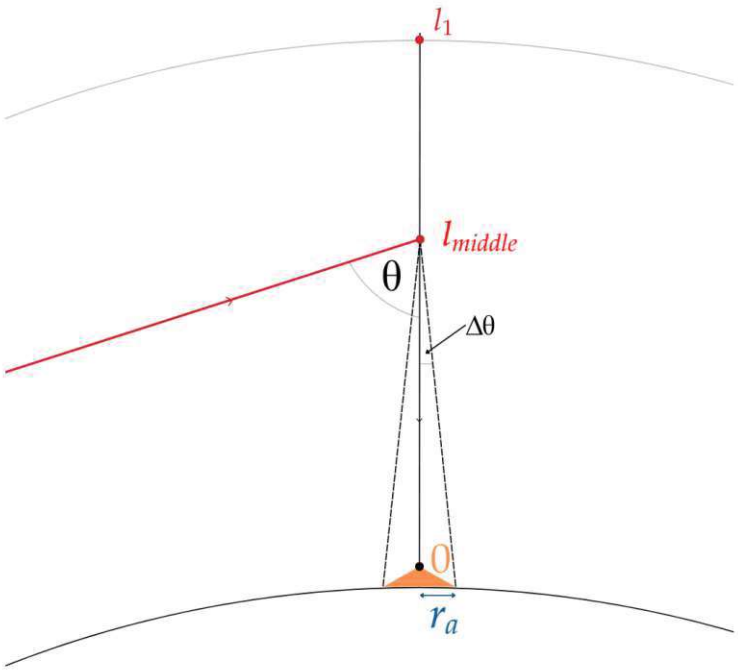

Figure 5.9: Visualization of the sun beam's path through the atmosphere, including its scattering at point l_{middle} at an angle θ into the receiver at 0 with the radius r_a, taking into account the introduced approximations.

This leads to the integration limits $\theta - \Delta\theta$ and $\theta + \Delta\theta$, where θ is the same angle was used in the previous section for $\Phi(\theta)$. Since $\Phi(\theta)$ is independent of ϕ, we only need to determine $\Delta\phi$, meaning the range of ϕ. This can be calculated as $\Delta\phi = 2\,\Delta\theta$ and therefore

$$b = F_0\, C_{ext}(\lambda)\, \Delta\phi \int_{\theta-\Delta\theta}^{\theta+\Delta\theta} \Phi(\theta)\, \sin(\theta)\, d\theta \int_{l_0}^{l_1} \rho(h(l))\, e^{-\tau_\Sigma(l)}\, dl, \tag{5.24}$$

which yields b in units of [erg/(s cm^2 μm)]. This can be converted analog to Equation (5.19), to the units [(s cm^2 nm)$^{-1}$]. Additionally, we need to define a bandwidth for $\Delta\lambda$ for the wavelength λ and multiply it by b. The final unit that requires conversion is [1/cm^2]. This is necessary because we assume that the field of view can be represented as a line, corresponding to the line of sight. In reality, we would need to integrate over a volume rather than just a length dl in Equation (5.26). To accurately account for the field of view, we would need to integrate over the cone that describing it. As a simplifying assumption, we consider the field of view to always align with the area of the receiver. This area can be expressed as

$$A_{receiver} = \pi \cdot r_a^2, \tag{5.25}$$

which, due to its independence of the distance z, can be multiplied as a factor to b.
Taking all of this into account, we can derive a new equation for the number of photons per second reaching the receiver:

$$b[s^{-1}] = \frac{10^{-7} \cdot 10^{-3}}{E_{photon}(\lambda)}\, A_{receiver}\, \Delta\lambda \cdot F_0\, C_{ext}(\lambda) \cdot \Delta\phi \int_{\theta-\Delta\theta}^{\theta+\Delta\theta} \Phi(\theta)\, \sin(\theta)\, d\theta \int_{l_0}^{l_1} \rho(h(l))\, e^{-\tau_\Sigma(l)}\, dl. \tag{5.26}$$

6 Results and outcomes

In this section, the results, outcomes and plots are discussed, comparing them to expected values to verify consistency.

6.1 The total surface brightness

In order to find results for the total surface brightness dependent on the sun's angular position, the transmittance of the atmosphere for different positions of the sun was plotted in Figure 6.1. In this graph, the x-axis refers to the height above sea level, where the sun's rays cross the FOV (which happens at point l). Therefore, Figure 6.1 showcases the transmittance of the sunbeam related to the height of its path within the atmosphere.

The transmittance is zero for values of l lower than $l_0(\phi)$. Starting at said minimum value $l_0(\phi)$, the transmittance increases rapidly to approximately one, meaning absorption is negligible for high values of l. Depending on ϕ, meaning the sun's position, the height at which the transmittance starts to grow changes significantly. This observation can be found to be reasonable, considering the geometrical setup of the simulation.

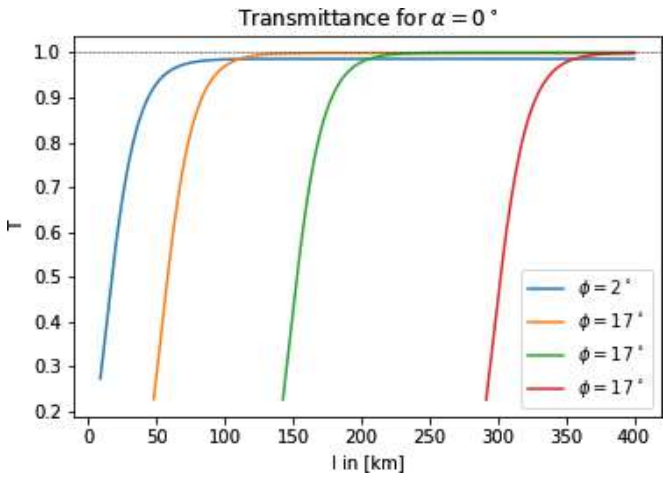

Figure 6.1: Transmittance on the entire path of the sunbeam, related to its height, with $\alpha = 0°$, for different angles ϕ. The x-axis shows the height at which the beam crosses the line of sight l. One can observe the transmittance to rapidly increase with increasing height of the path in the atmosphere.

From the transmittance in the atmosphere, the total surface brightness was calculated and shown in Figure 6.2. It is plotted against the different angles ϕ and the brightness is given in magnitudes per arcsecond squared. These units are not practical to estimate the noise in the receiver but can be utilized to compare the results to the results found by Patat et al. [29]. When comparing the figures, it is important to point out that the definition of the sun's angular position ϕ differs. In this thesis, ϕ corresponds to degrees below the horizon, while Patat et al. [29] define it as the angle related to the zenith. To properly compare these figures, 90° must be added to the ϕ utilized in this thesis. Additionally, it has to be pointed out, that the lowest calculated angle is $\phi = 2°$, since lower values of ϕ lead to numerical errors in the calculation.

One can observe the trajectory of the curve to be approximately constant until $\phi = 6°$, where it starts to decline, until it reaches its minimum at approximately $\phi = 14°$. For all of the following figures, the experimentally measured night sky brightness was added. Without that, the brightness would drop to zero for angles ϕ, for which no path through the atmosphere to the receiver is possible anymore. The same figure without the night sky brightness can be found in Appendix A.4. It can be concluded that for twilight stages $\phi \geq 14°$, the experimentally found night sky brightness is greater than the calculated brightness from single scattering events.

If one compares the results for different values of α, the differences between the curves are minimal. Especially for $\phi \leq 8°$, almost no difference can be observed. For greater values of ϕ, it can be seen that for negative α, meaning the line of sight points away from the sun, the b decreases faster toward the night sky brightness. Since a line of sight pointing away from the sun's direction should yield fewer photons in the receiver, this observation aligns with the expectations and is therefore reasonable.

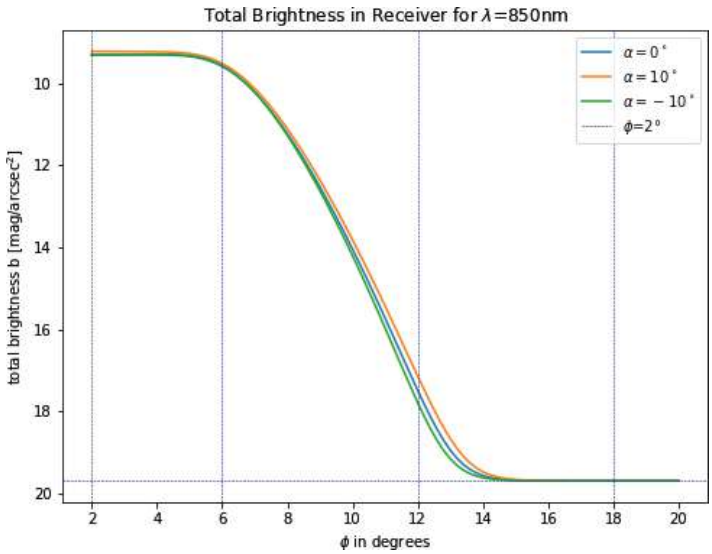

Figure 6.2: Total surface brightness b, in magnitudes per arcsecond squared for different angles α. The experimentally measured night sky brightness in included in this graph. The blue, dashed, vertical lines mark the end of civil, nautical and astronomical night.

In Figure 6.3, the calculated number of solar photons in [(s cm^2 μm arcsec^2)$^{-1}$] is presented. Overall, this result aligns with expectations. However, for the curve with $\alpha = -10°$, a slight increase in photon count is observed as ϕ increases. This outcome deviates from the expectations but can be explained by the assumption made. Only single scattering events were considered, and all scattering was modeled using the scattering phase function $\Phi(\theta)$, with the scattering angle θ. The scattering phase function is proportional to $(1 + \cos^2 \theta)$ (see Figure 5.8), with a minimum at $\theta = 90°$. In the assumed geometrical setup, θ ranges from 92° to 110° and increases with ϕ. This results in an increasing scattering phase function. As for low values of ϕ most other parameters are approximately constant, the effect of Φ becomes more apparent in this range. If additional effects, such as multiple-scattering events, were included, this increase would not be expected.

Another interesting observation is that after an almost constant behavior, the number of pho-

tons drops sharply at $\phi \approx 5°$, until it reaches its minimum, corresponding to the added night sky brightness at $\phi \approx 11°$. This suggests that the twilight brightness remains relatively constant during civil and astronomical twilight, but changes significantly during the nautical twilight stage.

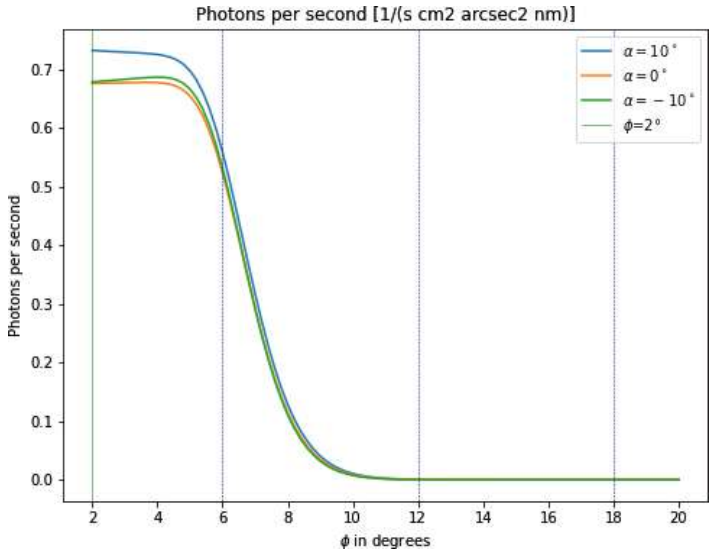

Figure 6.3: Photons per second cm^2, nm and arcsec^2, calculated from the total surface brightness b for different angles α. The blue dashed vertical lines indicate the end of civil, nautical, and astronomical night. It can be observed that for low angles of ϕ, the number of photons appears to increase for $\alpha \leq 0$. This observation results from the assumption that only single scattering and Rayleigh scattering, was taken into account.

As explained in Section 5.2.8, the expected number of photons reaching a receiver per second was calculated and is presented in Figure 6.4. As before, one can observe the approximately constant curve initially, where roughly 10^5 photons per second reach the receiver. During the subsequent twilight stages, this value decreases by six orders of magnitude until it reaches the constant night sky brightness.

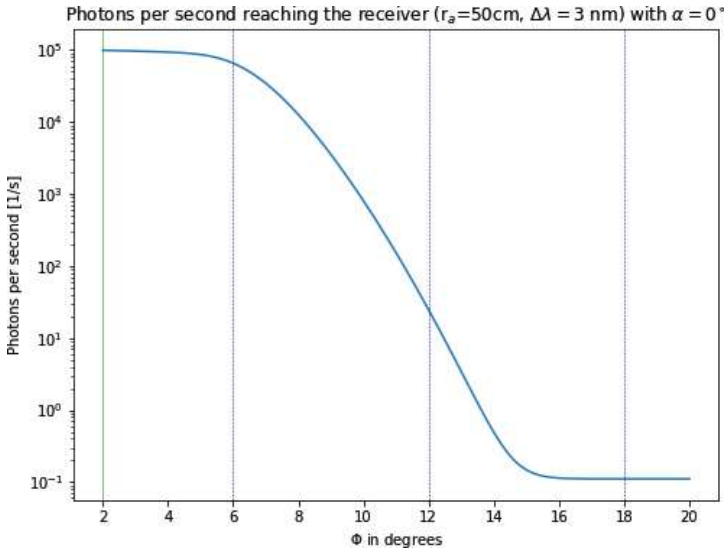

Figure 6.4: Number of photons per second reaching a realistic receiver for practical values. A bandwidth of $\Delta\lambda = 3\,\text{nm}$ was chosen for the wavelength, and the radius of the receiver aperture is selected to be $r_a = 50\,\text{cm}$. All necessary assumptions for this calculation can be found in Section 5.2.8.

6.2 Comparison of results to experimental data and literature

When comparing Figure 6.2 with the I-passband in Figure 5.1, one finds that the general distribution appears similar. Yet, some differences in the brightness behavior occur that require further examination [13]. Both curves are in the same range of brightness values, ranging from $b \approx 9\,\text{mag/arcsec}^2$ to $\approx 20\,\text{mag/arcsec}^2$. The constant behavior during civil twilight was not expected and thus has to be compared to experimental data and other models. In the calculated behavior for the I-passband by Patat et al. [29] does not exhibit this constancy, however, a reliable comparison is not possible, as the curve is only presented in the range of 4.5° to 20° below the horizon. Comparing the curves in this range is therefore not feasible.

As the calculations done in this thesis are based on the model by Patat et al. [29], the brightness is expected to reach night sky brightness at $\phi \approx 10°$. In contrast, the brightness found in this study reaches this value at $\phi \approx 14°$. Despite extensive efforts, this disagreement cannot be explained. Overall, it can be observed that the curve obtained this thesis is less steep than one anticipated. Figure 6.2 is in better agreement with the experimentally determined brightness by Patat et al. in Figure 5.1 than with the calculated brightness, even though the same assumptions were made. It can be concluded that the observed twilight brightness qualitatively aligns with expectations, although some differences remain unexplained.

To validate the simulated results, it is beneficial to compare them with data from other sources. To determine whether the order of magnitude by which the number of photons per second decreases during twilight is reasonable, Figure 6.4 was compared to Figure 5.3 by Barentine et al. [35] [14].

[13] Note that the angle ϕ is defined differently, as explained in Section 6.1.

[14] Barentine et al. used the same definition for ϕ as in this thesis, but with a sign change, meaning negative values for ϕ refer to twilight and night, while positive values refer to daylight.

In the latter figure the illuminance and its decrease during twilight are showcased in lux. Lux is defined as lumen per m^2, and lumen is defined as (cd · sr) with cd representing candela and sr referring to steradians [38]. As the aim of this section is to compare only the order of the decrease, the data can be directly compared without converting the units. In both figures, the number of photons is presented on a logarithmic scale, enabling a direct comparison of the two figures.

The first observation that can be made is that the constant behavior in early twilight stages, as previously noted, does not align with experimental findings. Furthermore, it can be observed that the brightness begins to decrease even before sunset, rapidly declining during civil and nautical twilight until it reaches the constant night sky brightness.

In Figure 5.3, one can see that the illuminance decreases from sunset to the end of astronomical twilight by about seven orders of magnitude [35]. Comparing that to the calculated plot for the number of photons per second, one can observe a decrease by approximately six orders of magnitude. There is only a difference of one order of magnitude, which is remarkable considering all assumptions and simplifications made in these calculations. Hence, one can conclude that the found results are considerably reasonable.

7 Simulation of key-rates for the BB84 decoy-state protocol

In order to gain a clearer understanding of the impact of the calculated results, it is helpful to calculate the key generation rate for different setups. To achieve this, the Decoy-state BB84 protocol, which employs two decoys: one with zero intensity and the other with non-zero intensity, was selected. The key generation rate calculation was computed following the methodology of Ma et al. [52]. However, this methodology presents key rates for fiber-based QKD channels. In order to obtain accurate results for free-space satellite QKD, the transmission efficiency was adjusted. Instead of the exponential decrease, which is typical for fiber, the loss calculations from Section 4 were employed.

7.1 Calculating the key generation rate for fiber-based QKD

To establish the lower bound of the key generation rate calculation, the expression

$$R \geq qQ_\mu \{ -H_2(E_\mu) + (1-\Delta)[1 - H_2(\frac{E_\mu}{1-\Delta})]\} \tag{7.1}$$

from Ma et al. [52] was utilized, where $q = \frac{1}{2}$ for all BB84 protocols and $H_2(x)$ is defined as

$$H_2(x) = -x\log_2(x) - (1-x)\log_2(1-x), \tag{7.2}$$

representing the binary Shannon information function [12]. Q_μ refers to the gain of the signal states as

$$Q_\mu = \sum_{i=0}^{\infty} Y_i \frac{\mu^i}{i!} e^{-\mu} = Y_0 + 1 - e^{-\mu\eta}, \tag{7.3}$$

and μ denotes the intensity of the signal states. E_μ describes the overall QBER. Δ is upper bounded by Wand [53] by the expression

$$\Delta \leq \frac{\mu}{\nu-\mu}\Big(\frac{\mu e^{-\mu} Q_\nu}{\nu e^{-\nu} Q_\mu} - 1\Big) + \frac{\mu e^{-\mu} Y_0}{\nu Q_\mu}, \tag{7.4}$$

and depends on μ, the intensity of the non-zero decoy signal ν, as well as Q_μ and Y_0, which refers to the background yield [52]. The background yield consists of dark counts in the detector and other photons reaching the receiver. Y_0 denotes the number of counts in the detector when the source is shut down [54].
To find the required overall gain Q_μ, it is necessary to determine η, the overall transmission and detection efficiency. Equation (7.3) shows the Poisson distribution of the number of photons sent in the weak coherent pulse. The overall transmission η is given by the product of the channel transmittance t_{AB} and the attenuation within Bob's receiver η_{Bob}. The transmission efficiency

$$t_{AB} = 10^{-\alpha z/10} \qquad \text{with } \alpha \text{ in [dB/km]} \tag{7.5}$$

demonstrates the typical exponential decrease over the link distance for fiber-based QKD. z again denotes the link distance. For free-space applications, said transmission must be determined differently.

The total QBER can be expressed as

$$E_\mu Q_\mu = \sum_{i=0}^{\infty} e_i Y_i \frac{\mu^i}{i!} e^{-\mu} = e_0 Y_0 + e_{detector}(1 - e^{-\mu\eta}), \tag{7.6}$$

with e_0 referring to the error in the vacuum. As these erroneous clicks happen at random, it can be concluded that $e_0 = \frac{1}{2}$.
For the protocol with two decoy states, consisting of one vacuum state and the other a weak decoy state ν, specifically where $\mu > \nu$.
To calculate the key rate R, additional parameters must be defined. The attenuation value α, the two intensities μ and ν, the background counts Y_0, the detection efficiency of Bob η_{Bob}, as well as the number of erroneous clicks in the detector $e_{detector}$.
When choosing the same values as Ma et al. [52], one finds the key generation rate to disappear at approximately 140 km link distance. These are reasonable values for fiber channels, but are anticipated to be significantly higher for free-space QKD [52].

W_0	Beam width at link distance $z = 0$	8 cm
q	Fixed for BB84 always:	1/2
μ	Signal state intensity	0.48
ν	Decoy state intensity	0.05
e_0	Background error rate (uncorrelated)	1/2
$e_{Detector}$	Probability that a signal photon produces erroneous click	0.03
η_{Bob}	Detector efficiency at Bob	0.85
R_a	Radius of the detection aperture	50 cm
Y_0	Background detection probability	$1.7 \cdot 10^{-6}$
f	Frequency of the pulses	2 MHz
$\Delta\tau/\Delta T$	Duty cycle	0.1

Table 7.1: Fixed input values used in the simulations. Some values were later varied to enhance the understanding of the behavior of the key generation rate R. Unless explicitly stated otherwise, the values above are utilized [52, 54]

7.2 Including noise induced by environmental photons from the sun during different twilight stages

In this section, the calculated key generation rates by Ma et al. [52] are adapted, while the subsequent calculations and analysis of noise have been developed as part of this thesis.
In order to demonstrate the impact of noise in the channel, the key generation rates will be plotted against the loss in dB, instead of the distance. This makes it possible to present the impact of noise without investigating loss contributions, which will be done in the next section.

To assess the impact of environmental photons from the sun on the noise in the channel, it is necessary to modify Y_0, as it refers to the background counts. This includes both the dark counts in the receiver and additional photons that may reach the detector.

The background yield Y_0 is the probability that a photon event is detected, although the source is shut down, meaning only vacuum states are sent. To account for the dark counts within the detector, we adopt an initial value for Y_0 of $1.7 \cdot 10^{-6}$, consistent with the findings of Ma et al. [52].

To find the background yield, including solar photons, we add this component to Y_0. In Figure 6.4, the number of photons from the sun reaching the receiver for a realistic receiver depending on the sun's angular position ϕ is illustrated. Said figure was derived by using Equation (5.26) for $b(\phi)$ in $[s^{-1}]$ [15], which we now employ as input to determine Equation (7.7) as follows. First, we consider the probability that a photon from the sun is measured, although a vacuum state was sent, by calculating the relation between the number of environmental photons per second reaching the receiver and the pulse frequency f. This relation must be multiplied by the receiver's efficiency η_{Bob} and the so-called duty cycle. This duty cycle refers to the fact that with an aligned receiver and source, the receiver is not detecting all the time, but only during the designated detection time $\Delta\tau$. This leads to shorter intervals in which environmental photons are effectively measured, thus reducing their contribution to the noise in the channel. Mitigating the noise contribution by reducing $\Delta\tau$ to negligible levels is impossible due to the timing jitter [54]. To calculate the duty cycle, one must divide $\Delta\tau$ by the period time ΔT of one pulse, which corresponds to the inverse of the frequency f. For the calculations in this thesis, the ratio $\Delta\tau/\Delta T = \Delta\tau \cdot f$ is selected to be either 0.1 or 1.
The preceding calculations result in Y_0^* being

$$Y_0^*(\phi) = Y_0 + \frac{b(\phi)}{f} \cdot \eta_{Bob} \cdot \frac{\Delta\tau}{\Delta T}. \tag{7.7}$$

Unless explicitly states otherwise, all parameters used in the calculations were selected as in Table 7.1.

7.3 Calculating the key generation rate for loss contributions

Once the noise contributions from the sun are included, it becomes important to include some contributions to the loss in the channel. In Section 4, the beam spread loss is calculated from the paraxial wave Equation [23]. The geometric efficiency $\eta_{geom}(z, r_a)$ describes the amount of the transmitted beam that reaches the receiver. In other words, it refers to the channel transmittance, assuming that beam spread loss is the only contribution to loss within the channel. Although atmospheric attenuation, turbulence or clouds are neglected, it yields a first impression of the impact of loss and noise on the channel. Therefore, it has to be noted that said model underestimates loss and thus results in longer link distances at which positive key rates can be achieved.

To apply the key generation rate calculations from Section 7.1, we alter the overall transmission η. It can be argued that all other parameters and assumptions do not rely on the channel, meaning fiber or free-space channels, hence can also be applied for our purposes. However, or the overall transmission for fiber channels

$$\eta = t_{AB} \cdot \eta_{Bob}, \tag{7.8}$$

the channel transmittance t_{AB} has to be replaced by $\eta_{geom}(z, r_a)$ as described in Equation (4.19), yielding the free-space transmission

$$\eta_{FS} = \eta_{geom}(z, r_a) \cdot \eta_{Bob}. \tag{7.9}$$

To enhance clarity, the geometric efficiency $\eta_{geom}(r_a, z)$ is converted to loss in [dB] as

[15] Note that the satellite was assumed to be at zenith ($\alpha = 0°$).

$$\text{Loss[dB]} = -10\, log_{10}\Big(\eta_{geom}(r_a, z)\Big), \tag{7.10}$$

and is illustrated in Figure 7.1.

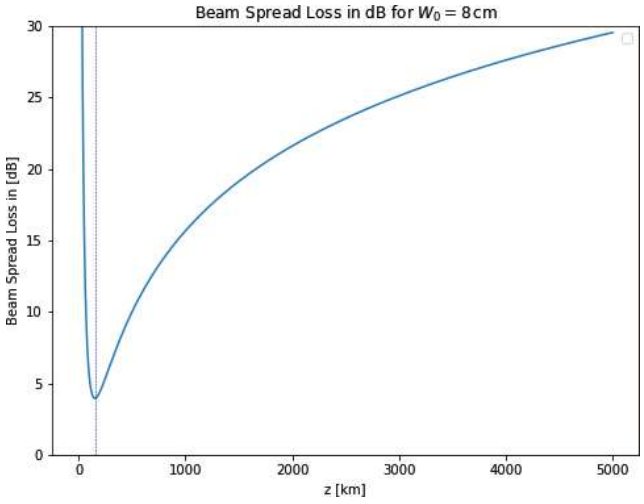

Figure 7.1: Beam spread loss $\eta_{geom}(z, r_a)$ as a function of the link distance z in [dB] with $W_0 = 8\,\text{cm}$, obscuration ratio $\gamma = r_{min}/r_a = 0.5$ and detection efficiency $\eta_{Bob} = 0.85$. Its high values for low distances results from the secondary mirror obscuring the center of the receiver as explained in Section 4. The vertical dashed line shows the minimum loss at $z_{min} = 151.95\,\text{km}$.

When investigating said figure, it can be seen, that at $z = 151.95\,\text{km}$, the beam spread loss is at its minimum. The high loss values for low z result from the obscuration due to the secondary mirror in the center of the telescope as described in Section 4. Since the minimum distance of a LEO satellite, to the ground station, is approximately 400 km [21], the key rates can reasonably be investigated for link distances $z \geq 152\,\text{km}$.

In the experiment by Liao et al. [14], the diffraction loss was assumed to be 22 dB at a link distance of 1200 km, which corresponds to the maximum. Comparing this value to the computed beam spread loss, it is found to be approximately 17.2 dB at 1200 km. This indicates an underestimation of the loss, however, it can be considered reasonable since not all diffraction loss was taken into account.

7.4 Key generation rate: results and comparison

In this section, the results and calculated key generation rates will be discussed.

As previously mentioned, before presenting the results, it is necessary to mention that all calculated maximum distances to extract positive key rates are overestimated, as only limited contributions to loss and noise were considered. Only one contribution to loss was assumed, as well as only solar photons and the night sky brightness were considered for the noise estimation. Further contributions to loss and noise that were not included, are for example atmospheric turbulence, city light, fog and many more.

Additionally, the underestimation of the sun's photons in the receiver, due to neglecting multiple-scattering events, leads to an additional underestimation of background noise and thus an overestimation of the key generation rate.
However, with that in mind, it is still valuable to investigate the calculated key rates to gain a better understanding of the general behavior.

7.4.1 Key generation rate: Results

Figures 7.2- 7.5 showcase the lower bound for the key generation rate per pulse R, for different values of the background noise Y_0. The various lines represent the key rates for different noise values as calculated in Equation (7.7). The blue line ($Y_0 = 0$) shows the key generation rate without any noise contributions. As they decrease exponentially, they consistently yield positive key rates, as expected. When background noise is added, it can be observed that R becomes ≤ 0 at some point. $Y_0(\phi = 2°)$ refers to the background counts within the receiver, which include photons from the sun when the sun's angular position is $\phi = 2°$ below the horizon. As expected, higher values of ϕ correspond to longer distances over which positive key rates can be maintained.

Figure 7.2 presents the key generations rates per pulse for a pulse frequency $f = 2\,\text{MHz}$ (as in [52]) and a duty cycle of $\Delta\tau/\Delta T = 0.1$. The maximum distances for successful key distribution, which represents the cutoff points, can be found in the range of 8 to 42 dB for $\phi = 2°$ TO $18°$. For comparison, the noise values Y_0 used in Figure 7.2 are showcased in Table 7.2.

In all figures, it can be seen that the night sky brightness contribution to noise leads to a maximum loss for positive key rates of approximately 42 dB, assuming a detector dark count yield of $Y_0 = 1.7 \cdot 10^{-6}$. For the different selected frequencies and duty cycles, this value does not change significantly. As for angles $\phi \geq 14°$ the night sky brightness exceeds the solar photons, the key generation rates for said angles, roughly align with the values for the night sky brightness.

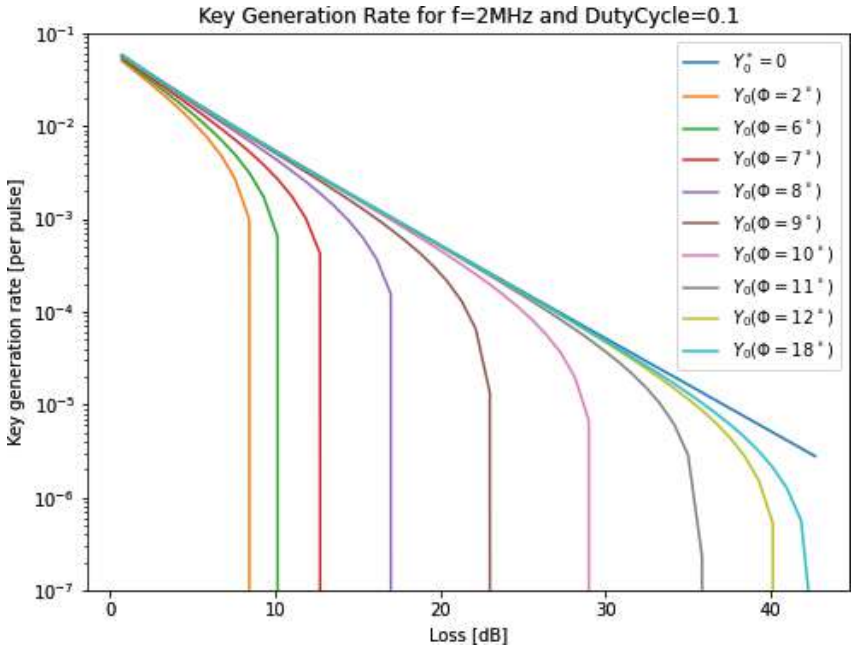

Figure 7.2: Key generation rate per pulse with frequency $f = 2\,\text{MHz}$ and duty cycle $\Delta\tau/\Delta T = 0.1$ for different noise due to solar photons $Y_0^*(\phi)$, for different sun's angular positions ϕ, plotted against the loss in [dB]. One can observe the key rate threshold declining for increasing background noise.

ϕ	$Y_0(\phi)$	$b(\phi)$ [s^{-1}]
2°	$4.21633752 \cdot 10^{-3}$	$9.91679417 \cdot 10^{4}$
3°	$4.11788543 \cdot 10^{-3}$	$9.68514218 \cdot 10^{4}$
4°	$3.97887486 \cdot 10^{-3}$	$9.35805849 \cdot 10^{4}$
5°	$3.68066632 \cdot 10^{-3}$	$8.65639133 \cdot 10^{4}$
6°	$2.79306922 \cdot 10^{-3}$	$6.56792758 \cdot 10^{4}$
7°	$1.46922791 \cdot 10^{-3}$	$3.45300684 \cdot 10^{4}$
8°	$5.39639024 \cdot 10^{-4}$	$1.26573888 \cdot 10^{4}$
9°	$1.51849511 \cdot 10^{-4}$	$3.53292967 \cdot 10^{3}$
10°	$3.57631737 \cdot 10^{-5}$	$8.01486441 \cdot 10^{2}$
11°	$8.16925204 \cdot 10^{-6}$	$1.52217695 \cdot 10^{2}$
12°	$2.74060527 \cdot 10^{-6}$	$2.44848299 \cdot 10^{1}$
13°	$1.84496151 \cdot 10^{-6}$	$3.41085913 \cdot 10^{0}$
14°	$1.72071660 \cdot 10^{-6}$	$4.87449418 \cdot 10^{-1}$
15°	$1.70623698 \cdot 10^{-6}$	$4.87449418 \cdot 10^{-1}$
16°	$1.70482223 \cdot 10^{-6}$	$1.13464249 \cdot 10^{-1}$
17°	$1.70470665 \cdot 10^{-6}$	$1.10744728 \cdot 10^{-1}$
18°	$1.70469878 \cdot 10^{-6}$	$1.10559555 \cdot 10^{-1}$

Table 7.2: Background yield Y_0 and photons per second reaching the receiver $b(\phi)$ for $\lambda = 850\,\text{nm}$, $f = 2\,\text{MHz}$ and duty cycle $\Delta\tau/\Delta T = 0.1$ for different sun's angular positions ϕ, along with the assumed background detector noise $Y_0 = 1.7 \cdot 10^{-6}$. The corresponding key generation rates are shown in Figure 7.2.

When comparing the key rates for different background noise values in Figure 7.2 to the previously calculated twilight sky brightness, one can observe the same rapid change in the brightness, respectively solar photon noise. The key rate cutoff varies by 3 dB for $\phi = [2°, 6°]$ before increas-

ing from approximately 10 dB to nearly 35 dB in the range $\phi = [6°, 12°]$. During the subsequent astronomical twilight, only marginal changes in the key rate cutoff can be observed.

In order to gain a better understanding of the impact of the different parameters, the duty cycle was set to = 0 in Figure 7.3. Compared to the previous figure, one finds a drastic decline in the loss threshold. For values of ϕ lower than 6°, key generation cannot be achieved at all. For $Y_0(\phi)$, where positive key rates can be achieved, the key rate cutoff points are significantly worse than for a duty cycle of 0.1. Consequently, one observes a severe impact of the measuring time of the receiver.

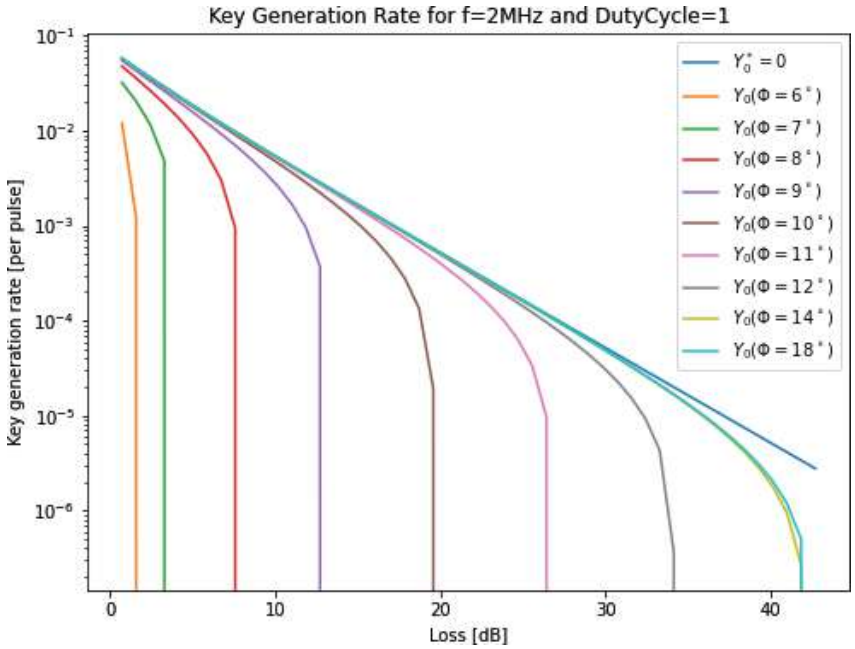

Figure 7.3: Key generation rate per pulse with frequency $f = 2$ MHz and duty cycle $\Delta\tau/\Delta T = 1$ for different noise due to solar photons $Y_0^*(\phi)$, for different sun's angular positions ϕ, plotted against the loss in [dB].

Additionally, the pulse frequency f can be varied. For the Figures 7.4 and 7.5, the frequency was increased to $f = 1$ GHz, leading to two key observations. First, the key rate threshold increases significantly compared to the previously utilized pulse frequency. Second, the impact of the sun's position declines, with all cutoff points now found in the range of 26 dB up to 43 dB for a duty cycle of $\Delta\tau/\Delta T = 1$ (Figure 7.4). Said figure also suggests that even for angles just below the horizon, positive key rates may be obtained for loss up to 26 dB, which is not expected for realistic implementations. Thus, one can conclude that for $f = 1$ GHz, the key generation rate is significantly overestimated in these results.

Reducing the duty cycle to $\Delta\tau/\Delta T = 0.1$, while keeping the frequency $f = 1$ GHz, it can be noticed that the key generation rates R improve further. The impact of solar photons diminishes even more. It can be stated that Figure 7.5 does not yield reasonable outcomes for free-space satellite QKD.

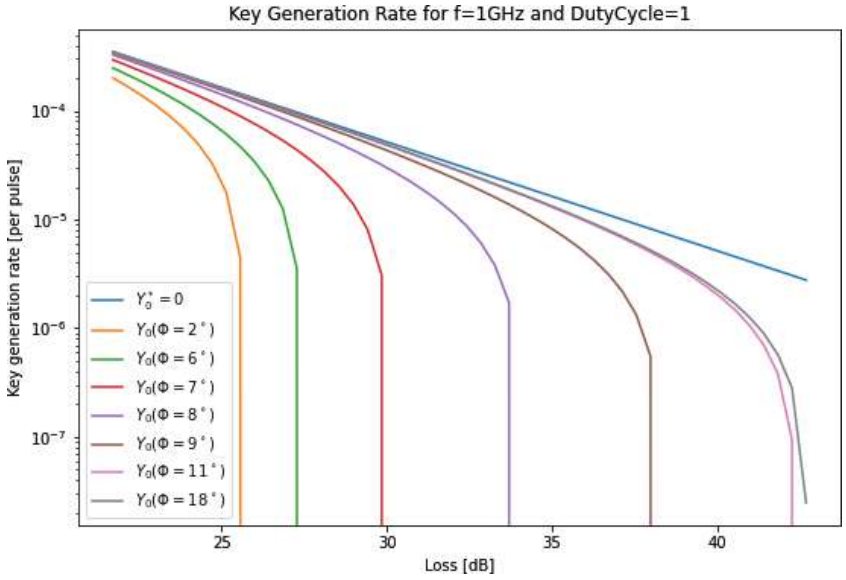

Figure 7.4: Key generation rate per pulse with frequency $f = 1\,\text{GHz}$ and duty cycle $\Delta\tau/\Delta T = 1$ for different noise due to solar photons $Y_0^*(\phi)$, for different sun's angular positions ϕ, plotted against the loss in [dB].

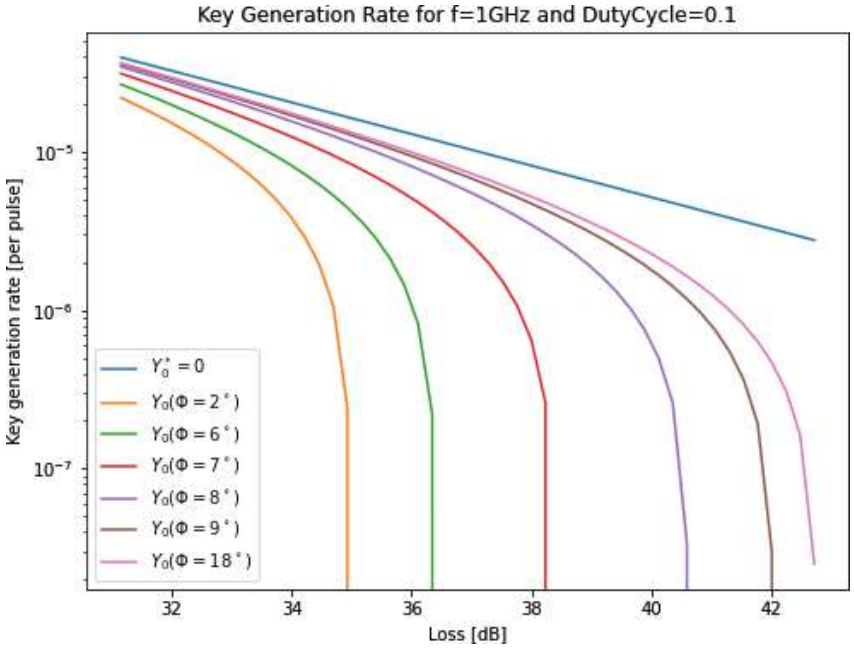

Figure 7.5: Key generation rate per pulse with frequency $f = 1\,\text{GHz}$ and duty cycle $\Delta\tau/\Delta T = 0.1$ for different noise due to solar photons $Y_0^*(\phi)$, for different sun's angular positions ϕ, plotted against the loss in [dB].

It can be concluded that the qualitative behavior of the key generation rate per pulse is plausible. However, the results vary depending on the input parameters, some calculated results may not be reasonable and realistic results.

7.4.2 Key generation rate: Results for free-space Sat-QKD including beam spread loss

In this section, the calculations for loss and noise are combined and integrated. The same key generation rates for different twilight stages as in Section 7.4.1 are now displayed in relation to the link distance z, calculated in Section 7.3.

To interpret the figures, it is useful to recall prior results. The beam spread loss was calculated with a maximum link distance of 5000 km. The loss at that distance z is calculated to be about 30 dB. Therefore, the key rate cutoff points over 30 dB are not shown in the following plots.

Since the secondary mirror is obscuring the center of the receiver (see Section 4 obscuration ratio), the loss is decreasing in the range from 0 to 151 km. To obtain reasonable results, this range was excluded in these figures. Given that the minimum distance between the satellite and the receiver is 400 km, this assumption is valid.

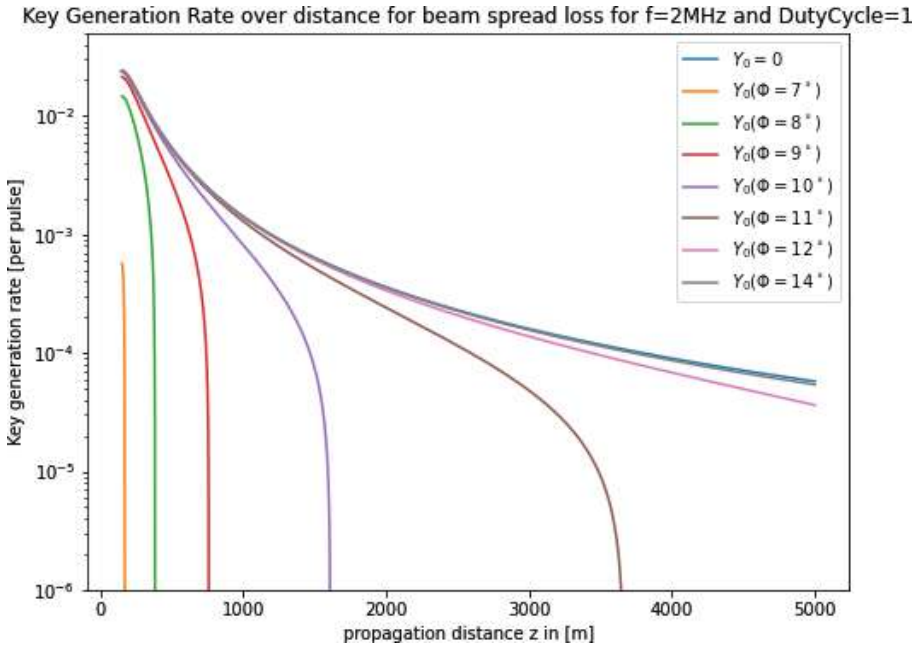

Figure 7.6: Key generation rate per pulse related to the link distance z in km, at a frequency of $f = 2\,\text{MHz}$ and a duty cycle $\Delta\tau/\Delta T = 1$, with varying noise contributions from solar photons $Y_0^*(\phi)$ at for different solar angular positions ϕ.

Figure 7.6 displays the key rate cutoff points as a function of the link distance for $f = 2\,\text{MHz}$ and $\Delta\tau/\Delta T = 1$. For $\phi = 7°$ and $8°$, no key distribution can be achieved for any LEO satellite overpass, since their cutoff points are at $z \approx 172\,\text{km}$ and $383\,\text{km}$ respectively, both of which are lower than the minimum link distance of a LEO satellite. For higher values of ϕ, the key rate threshold also increases markedly, with possible link distances exceeding the observed range for $\phi \leq 12°$. With

said parameters and solar photons noise $Y_0(\phi = 18°)$, the cutoff point would be nearly 19 000 km, which is drastically overestimated. Also, it is important to note that this calculated was made with parameters that yield the lowest key generations rates.

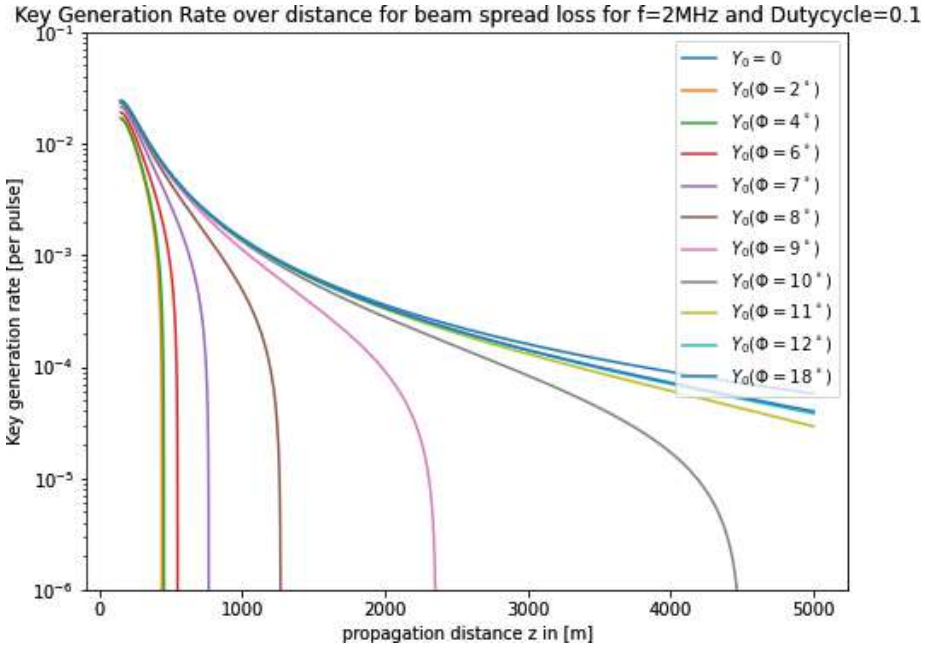

Figure 7.7: Key generation rate per pulse related to the link distance z in km, at a frequency of $f = 2\,\text{MHz}$ and a duty cycle $\Delta\tau/\Delta T = 0.1$, with varying noise contributions from solar photons $Y_0^*(\phi)$ at for different solar angular positions ϕ.

When adjusting the duty cycle to be 0.1, it is clear that during a typical overpass of a LEO satellite, key distribution can be achieved for the entire duration of the overpass for $\phi \leq 10°$, given that the maximum link distance z of a LEO satellite overpass is about 3000 km. For $\phi = [2°, 9°]$, key generation can be achieved up to a certain distance in the range of a satellite overpass.

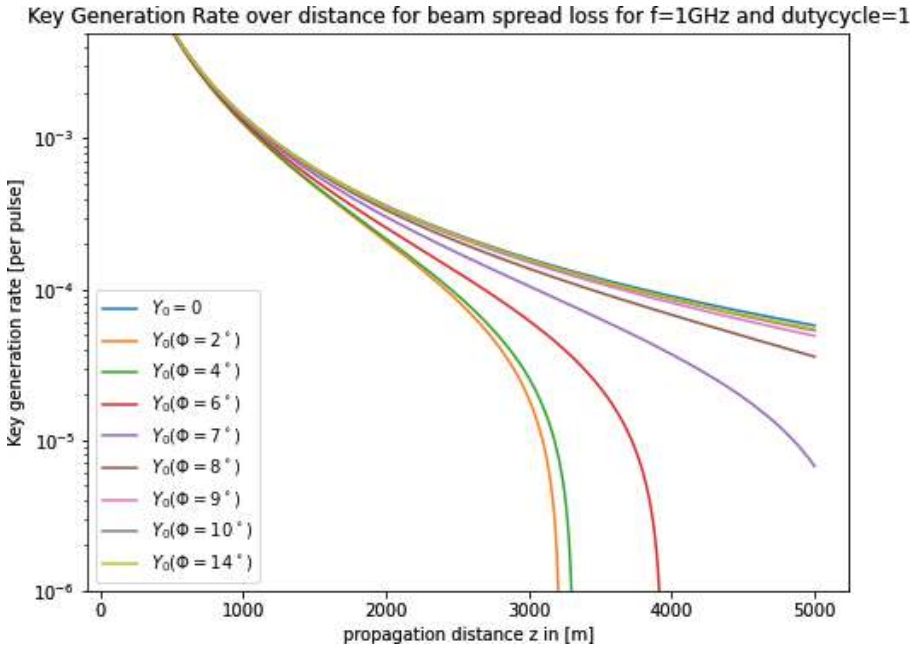

Figure 7.8: Key generation rate per pulse related to the link distance z in km, at a frequency of $f = 1\,\text{GHz}$ and a duty cycle $\Delta\tau/\Delta T = 1$, with varying noise contributions from solar photons $Y_0^*(\phi)$ at for different solar angular positions ϕ.

Increasing the frequency to $f = 1\,\text{GHz}$, with $\Delta\tau/\Delta T = 0.1$, leads to maximum key distribution distances z exceeding 3000 km across all investigated values of ϕ. Thus, it can be concluded that the simulation with said parameters does not adequately represent the key generation rates per pulse for the free-space satellite QKD decoy-state protocol.

8 Conclusion and outlook

This thesis aimed to model loss and noise in satellite free-space quantum key distribution during twilight stages and their impact on achievable key generation rates.

A basis for the following calculations was developed by successfully reproducing an already existing model to describe the twilight sky brightness. Even though results show small deviations from the existing model, they align well with experimental data. For the purpose of extending the model to describe solar photons per second reaching a realistic receiver in a downlink setup, further calculations were necessary.

Neglecting various other loss contributions, the beam spread loss in free-space satellite QKD was simulated as a representative example. The performed simulations provide a sufficient basis for calculating key generation rates, related to the impact of loss and noise on the channel.

To estimate the key generation rates for different twilight stages, a decoy-state BB84 protocol was taken into account. The protocol was adapted to apply to free-space QKD instead of fiber. We included the results found in the previous solar photon noise calculations and obtained reasonable key generation rates for different twilight stages.

Investigating the outcomes, the key rate cutoffs appear to be accurate and align with initial expectations. Furthermore, the choice of the pulse frequency and the duty cycle were found to severely impact achievable key rates. Comparing the data to key rates obtained in free-space experiments conducted at night, one can conclude that the model overestimates the key rate values. This stems from the underestimation of loss and noise in the previous simulations.

To mitigate the resulting overestimation, including multiple-scattering events in the solar photon noise calculations is advantageous. An interesting improvement is the generalization to a three-dimensional geometrical model, to enable an accurate description of a LEO satellite's overpass.

Conclusively, the simulated model developed in this thesis can be considered an accurate basis for describing loss and solar photon noise in free-space quantum key distribution during twilight stages.

A Appendix

Additional information, details, and figures are presented below.

A.1 The Gaussian beam - The paraxial approximation

In Section 4.1, the calculation of the Gaussian beam by Andrews et al. [23] is presented. It employs the *paraxial approximation*, which is explained in the following.

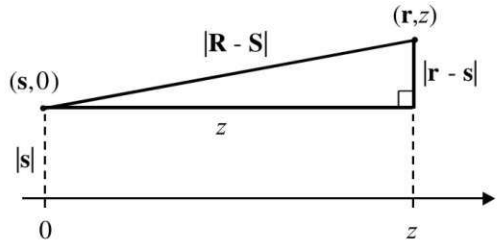

Figure A.1: Geometric visualization of the paraxial approximation, with the source of the beam at 0 and z denoting the link distance. Taken from [23].

It assumes that the longitudinal propagation distance z is much larger than transverse distance $|\mathbf{r}-\mathbf{s}|$. In this calculation $\mathbf{s}$ refers to the transverse distance to the optical axis at link distance $z = 0$, as visualized in Figure A.1. $\mathbf{R}$ and $\mathbf{S}$ correspond to two points in space, with $\mathbf{r}$ and $\mathbf{s}$ being the transverse components of these points with

$$|\mathbf{R}-\mathbf{S}| = (z^2 + |\mathbf{r}-\mathbf{s}|^2)^{1/2} = z\Big(1 + \frac{|\mathbf{r}-\mathbf{s}|^2}{z^2}\Big)^{1/2}. \tag{A.1}$$

As one assumes $z << |\mathbf{r}-\mathbf{s}|$, Equation (A.2) can be developed in a Taylor series to be

$$|\mathbf{R}-\mathbf{S}| = z + \frac{|\mathbf{r}-\mathbf{s}|^2}{2z} + ... \tag{A.2}$$

The paraxial approximation now is only taking into account the first two terms in the above equation. To employ the approximation, one must simplify Equation (4.3) with $U_0(r,z) = V(r,z)e^{ikz}$ to

$$\frac{1}{r}\frac{\partial}{\partial r}\Big(r\frac{\partial V}{\partial r}\Big) + \frac{\partial^2 V}{\partial z^2} + 2ik\frac{\partial V}{\partial z} = 0 \tag{A.3}$$

and finds

$$\Big|\frac{\partial^2 V}{\partial z^2}\Big| \ll \Big|2k\frac{\partial V}{\partial z}\Big| \qquad \text{and} \qquad \Big|\frac{\partial^2 V}{\partial z^2}\Big| \ll \Big|\frac{1}{r}\frac{\partial}{\partial r}\Big(r\frac{\partial V}{\partial r}\Big)\Big|. \tag{A.4}$$

Therefore, it can be argued that with $\frac{\partial^2 V}{\partial z^2} = 0$, Equation (A.3) results in

$$\frac{1}{r}\frac{\partial}{\partial r}\Big(r\frac{\partial V}{\partial r}\Big) + 2ik\frac{\partial V}{\partial z} = 0, \tag{A.5}$$

which corresponds to Equation (4.4) [23].

A.2 Geometric calculations

Below the geometrical calculations to find h_{QP} shown in Equation (5.1) are presented in more details.
As illustrated in Figure 5.5, one assumes an optical receiver located at O, at height above sea level h_s. h_s is restricted to be $< 3\,\text{km}$, to maintain the applied assumption that the horizon is a flat line through O. The field of view (FOV) is assumed to be the line of sight (LOS), meaning the opening angle of the FOV is 0°. The position of the sun is described by the angle ϕ, with $\phi = 0$ representing the sun at the horizon, corresponding to the sun being an angle of 90° related to the zenith. The range of the sun's angular position ϕ investigated by Patat et al. [29] expands from 4° to 22°. The range of interest for this thesis is 2° to 18°. The geometrical calculations are not restricted to said range, however, are not investigated for exceeding values of ϕ.
The direction of the line of sight is defined by α, which denotes the angle of the LOS related to the zenith. Positive angles of α point in the direction of the sun, negative values point in the opposite direction. In the paper by Patat et al. [29] only positive values were discussed.

Additionally, it should be noted that due to geometrical calculations the simulation does not apply to arbitrary values of α, but is restricted to a maximum angle of $|\alpha_{max}|$, depending on ϕ. Said maximum angle is found in the range of approximately 20° for small values of ϕ to $|\alpha_{max}| \approx 73°$ for $\phi = 18°$. When further increasing ϕ, one finds that at a certain angle no path through the atmosphere to the line of sight is possible anymore, which results in a brightness of 0 at the receiver. For the total brightness calculations the experimentally found night sky brightness was added, which leads to the non-zero brightness even for angles lower than the maximum ϕ.
The calculation works as follows. First, one can find the distance between H_0 and P_0 as

$$H_0P_0 = R_0\Big[\,\tan(\phi) - \frac{\sin(\alpha)}{\cos(\alpha-\phi)}\left(\frac{1-\cos(\phi)}{\cos(\phi)} - \frac{h_s}{R_0}\right)\Big]. \tag{A.6}$$

H_0P_0 only depends on α and ϕ, while the distance HP also depends on l, meaning it requires l as an input parameter and is written as

$$HP = H_0P_0 - (\,l - l_0\,)\,\sin(\alpha-\phi). \tag{A.7}$$

Then one has to calculate h_0, which describes the height above sea level of P_0 as

$$h_0 = \sqrt{H_0P_0^2 + R_0^2} - R_0. \tag{A.8}$$

To find all possible values of l for fixed α and ϕ, one calculates the minimum l_0 and the maximum l_1 of l as

$$l_0 = \sqrt{(R_0+h_s)^2\,\cos(\alpha)^2 + h_0^2 - h_s^2 + 2R_0\,(h_0-h_s)} - (R_0+h_s)\,\cos(\alpha) \qquad \text{and} \tag{A.9}$$

$$l_1 = \sqrt{(R_0+h_s)^2\,\cos(\alpha)^2 + 2R_0\,(\Delta R - h_s) + \Delta R^2 - h_s} - (R_0+h_s)\,\cos(\alpha). \tag{A.10}$$

To calculate h_{QP}, one needs to calculate δ, which is expressed as

$$\delta = (\,l - l_0\,)\,\cos(\alpha-\phi). \tag{A.11}$$

Utilizing the equations above, one finds the distance QH as

$$QH = \sqrt{2R_0\,(\Delta R - \delta) + \Delta R^2 - \delta^2}. \tag{A.12}$$

With these in mind, one can calculate the height asl h_{QP} for every point on the beam's path. Therefore, q is defined with $q = 0$ at Q, expanding to QP. Utilizing the equations above, a function is defined, which requires α and ϕ, but also l and q as input parameters, which is

$$h_{QP} = \sqrt{(QH - q)^2 + (R_0 + \delta)^2} - R_0, \tag{A.13}$$

and align with Equation (5.1) in Section 5.

Additionally, to calculate the fraction of the beam that scatters at an angle θ_R, which denotes the scattering angle that leads to the beam reaching the receiver, corresponding to scattering in the field of view, has to be found:

$$\theta_R = 90° - \alpha - \phi. \tag{A.14}$$

For a better understanding of the beam's path, the height asl h_{QP} for fixed angles $\alpha = 1°$ and $\phi = 6°$ is illustrated in Figure A.2 [29].

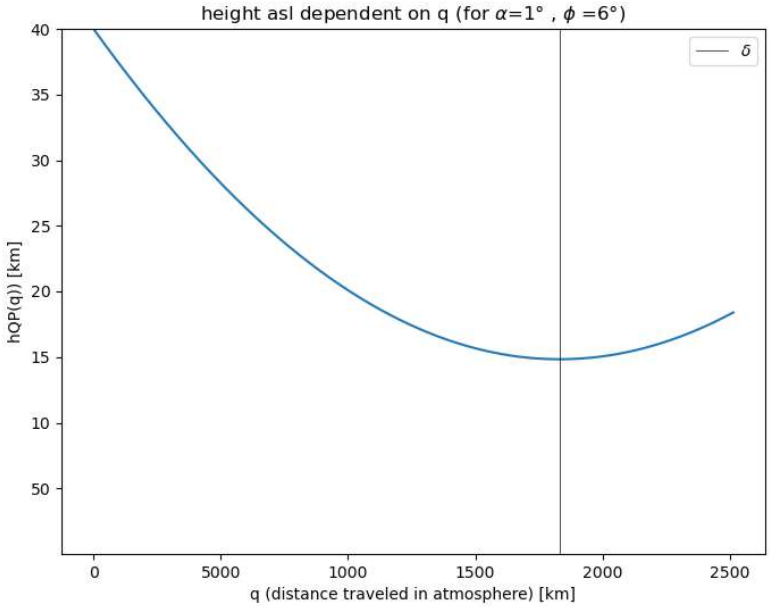

Figure A.2: Height above sea level h_{QP} on the beam's path through atmosphere. The vertical line is representing the point H, at which the height asl is at its minimum, corresponding to the height asl δ.

A.2.1 Approving negative values for α

Although Patat et al. [29] did not discuss the geometrical setup for negative angles α, it was proven that the calculations also hold for said angles, as part of this thesis.

We recalculate l_0 and l_1 to be

$$l_0 = (R_0 + h_0) \cdot \frac{1}{\sin\alpha} \cdot \sin\Big(\alpha - \arcsin\Big(\frac{R_s}{R_0 + h_s} \cdot \sin\alpha\Big)\Big) \qquad \text{and} \tag{A.15}$$

$$l_1 = \frac{R_0 + \Delta R}{\sin\alpha} \cdot \sin(\alpha - \epsilon), \qquad \text{with} \tag{A.16}$$

$$\epsilon = \arcsin\Big(\frac{R_0 + h_s}{R_0 + \Delta R} \cdot \sin\alpha\Big). \tag{A.17}$$

These yield the same results as the equations presented by Patat et al. [29], thus can be assumed to be reasonable.

A.2.2 Density distribution of scattering particles in the atmosphere

In Figure A.3 the density distribution $\rho(q)$ along the beam's path through the atmosphere q is visualized, which depends on α, ϕ and l. They were selected arbitrarily, with $\alpha = 0°$, meaning the FOV points directly to the zenith. Since we are interested in twilight brightness, therefore small angles related to the horizon, $\phi = 6°$ was selected for the figure. l was defined as the average of l_0 and l_1 for said α and ϕ.

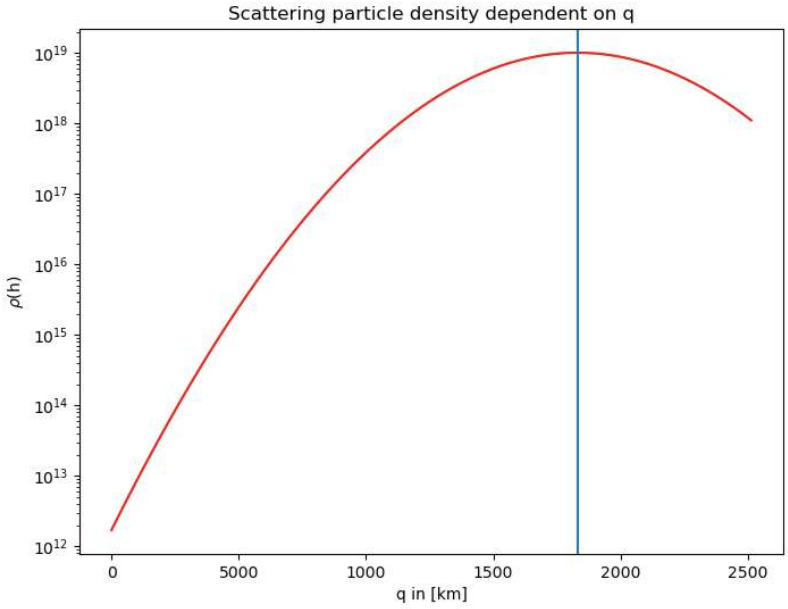

Figure A.3: Density distribution ρ over the path q through atmosphere for $\phi = 6°$, $\alpha = 0°$.

A.3 Calculating the sun's luminosity utilizing Planck's radiation law

In the following, the ansatz to calculate the number of photons independently of the experimentally found zeropoints, is presented. However, it was not possible to find reasonable values for the sun's luminosity. As it is considered an interesting approach, it is presented below, nevertheless.

In order to find the number of photons from the sun for arbitrary wavelengths λ and arbitrary bandwidths $\Delta\lambda$, the sun is assumed to be a perfect black body with temperature $T = 5772\,\mathrm{K}$, which equals the surface temperature of the sun. Due to this approach, the Planck's radiation law can

be utilized, which is the quantum mechanical description of radiation and its distribution of the wavelength and temperature. It is defined as

$$u(\lambda, T) = \frac{8\pi hc}{\lambda^5} \cdot \frac{1}{e^{\frac{hc}{\lambda k_B T}} - 1}, \tag{A.18}$$

and is the energy density of a black body, including the Bose-Einstein distribution for bosons, meaning for particles with integer spin[16] and is given as energy per unit volume and unit wavelength [55].
However, for these calculations one needs the number of photons per second and not energy per volume. Therefore, the function will be utilized as a method to describe the energy distribution of the sun. One integrates over all wavelengths from 0 to infinity, and states that is must be one. Thus, an additional factor corresponding to a normalization constant n, must be included as

$$n \cdot U(T) = n \int_0^\infty u(\lambda, T)\, d\lambda = 1, \tag{A.19}$$

and one finds $n = 1.19082$. With that in mind, one can now decide which bandwidth $\Delta\lambda$ is required and calculate the fraction of the entire energy of the sun that is given by the selected wavelength range $p(\lambda, \Delta\lambda)$, as

$$p(\lambda, \Delta\lambda) = n \cdot u(\lambda, T) \cdot \Delta\lambda. \tag{A.20}$$

It is worth noting that the above equation is only suitable for small values of $\Delta\lambda$, since the energy distribution in that range, is here assumed to be constant. For bigger bandwidths, one needs to integrate over the required bandwidth $d\lambda$. For $\lambda = 850\,\text{nm}$ and $\Delta\lambda = 1\,\text{nm}$ this fraction is found to be $p(\lambda, \Delta\lambda) = 0.0007$. To find the power of the sun for said bandwidth, one multiplies $p(\lambda, \Delta\lambda)$ by the total power of the sun $P_{tot} = 3.846 \cdot 10^{26}\,\text{W}$ [56].
To calculate the number of photons emitted per second in the required wavelength range, one calculates the energy of one photon with a certain wavelength λ as

$$E(\lambda) = \frac{hc}{\lambda}. \tag{A.21}$$

Utilizing this equation, one divides the power emitted in the range $\Delta\lambda$ by the energy of one photon with λ. This results in the following number of photons per second:

$$N(\lambda, \Delta\lambda) = \frac{p(\lambda, \Delta\lambda) \cdot P_{tot}}{E(\lambda)}. \tag{A.22}$$

For the values selected for these calculations, one finds that $N(\lambda = 850\,\text{nm}, \Delta\lambda = 1\,\text{nm}) = 1.2405 \cdot 10^{42}$. To calculate F_0, $N(\lambda = 850\,\text{nm}, \Delta\lambda = 1\,\text{nm})$ has to be divided further by $4\pi d^2$. This yields $F_0 = 4.3873 \cdot 10^{18}\,(\text{s cm}^2\ \text{nm})^{-1}$, which does not align with the values obtained in Section 5.2.5. The aim to calculate sun's luminosity, therefore, cannot be accomplished utilizing the above calculations.

A.4 Brightness Calculations

In Section 5.2.7 the total brightness is calculated. In the following, additional details are presented [29].

[16] The photon's spin is zero.

An infinitesimal volume element dV within the line of sight, respectively field of view, is assumed to find df, referring to "the number of scattered photons received by he observer per unit time, unit area, and unit wavelength" [17] as

$$df = F_0\, e^{-\tau_{QP}}\, \rho[h(l)]\, C_{ext}(\lambda)\, \frac{\Phi(\theta)}{l^2}\, e^{-\tau_{0P}}\, dV. \tag{A.23}$$

The volume dV equals $dS\, dl$, with dl representing the direction along l and $dS = \pi l^2 \phi^2$. The angle ϕ describes the "semi-amplitude of the angle subtended by dS at the distance of the observer" [29], and not the sun's angular distance. With $dS = \pi\phi^2$ denoting the solid angle, one can rewrite the equation to find the surface brightness db produced by the volume element dV to be

$$db = \frac{df}{d\Omega} = F_0\, e^{-\tau_{QP}}\, \rho[h(l)]\, C_{ext}(\lambda)\, \Phi(\theta)\, e^{-\tau_{0P}}\, dl. \tag{A.24}$$

Using db, which represents the brightness from an infinitesimal element dl, one can calculate the total surface brightness by $b = \int_{l_0}^{l_1} db$, by integrating over all possible paths for the sun ray through the atmosphere, which results in the integration limits of l_0 and l_1.
To find the total brightness, one calculates

$$b = F_0\, C_{ext}(\lambda)\, \Phi(\theta) \int_{l_0}^{l_1} \rho(h(l))\, e^{-(\tau_{QP} + \tau_{0P})}\, dl, \tag{A.25}$$

which is done numerically in this thesis [29].

A.5 Results: Twilight sky brightness

In Figure A.4, the calculated twilight sky brightness without the added experimentally found night sky brightness is presented.

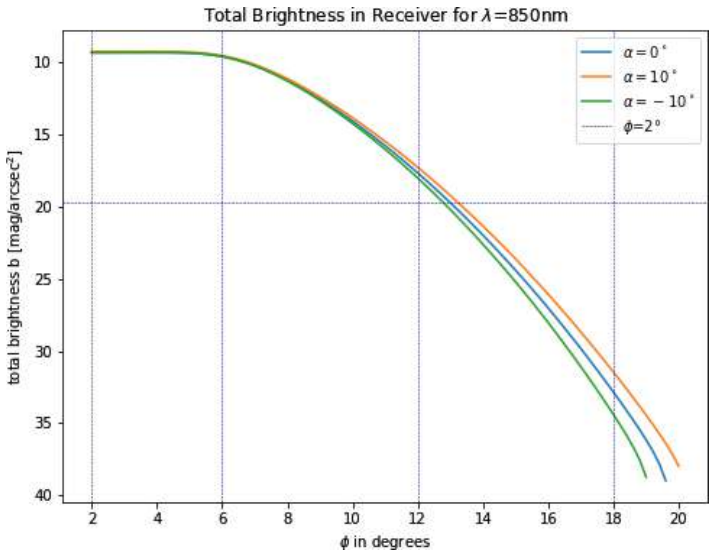

Figure A.4: Total surface brightness b, in magnitudes per arcsecond squared for different angles α, without the experimentally measured night sky brightness. The blue, dashed, vertical lines mark the end of civil, nautical and astronomical night. The blue, dashed, horizontal line shows the night sky brightness.

[17] Note that, τ_{QP} and τ_{OP} could be combined in τ_Σ, but in this section, the notation by Patat et al. [29] is followed

In Figure 6.2 in Section 6, the same brightness is illustrated, but is including the night sky brightness. When comparing these figures, one can observe a significant deviation for angles of $\phi < 14°$. The calculated twilight sky brightness declines to zero, without the added night sky brightness, which is reasonable due to the geometrical setup.

A.6 Data: The UBVRI passbands

In the following table, the values of the UBVRI passbands are showcased.

		U	B	V	R	I
Zeropoint	M_0	-10.93	-10.5	-11.05	-11.90	-12.70
Sun's Magnitude	M_{sun}	-25.96	-26.09	-26.74	-27.26	-27.55
Night sky Brightness	M_{night}	22.3	22.6	21.6	20.9	19.7

Table A.1: Data for the UBVRI passbands in magnitudes. Taken from [39, 40].

References

[1] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J Cerf, Miloslav Dušek, Norbert Lütkenhaus, and Momtchil Peev. The security of practical quantum key distribution. *Reviews of modern physics*, 81(3):1301–1350, 2009.

[2] CH Ugwuishiwu, UE Orji, CI Ugwu, and CN Asogwa. An overview of quantum cryptography and shor's algorithm. *Int. J. Adv. Trends Comput. Sci. Eng*, 9(5), 2020.

[3] Daniel J Bernstein and Tanja Lange. Post-quantum cryptography. *Nature*, 549(7671):188–194, 2017.

[4] Renato Renner and Ramona Wolf. Quantum advantage in cryptography. *AIAA Journal*, 61(5):1895–1910, 2023.

[5] Valerio Scarani and Christian Kurtsiefer. The black paper of quantum cryptography: real implementation problems. *Theoretical Computer Science*, 560:27–32, 2014.

[6] Feihu Xu, Xiongfeng Ma, Qiang Zhang, Hoi-Kwong Lo, and Jian-Wei Pan. Secure quantum key distribution with realistic devices. *Reviews of modern physics*, 92(2):025002, 2020.

[7] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. Quantum cryptography. *Reviews of modern physics*, 74(1):145, 2002.

[8] Ronald L Rivest, Adi Shamir, and Leonard Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.

[9] Normand J Beaudry. Assumptions in quantum cryptography. *arXiv preprint arXiv:1505.02792*, 2015.

[10] Gilbert S Vernam. Cipher printing telegraph systems: For secret wire and radio telegraphic communications. *Journal of the AIEE*, 45(2):109–115, 1926.

[11] Claude E Shannon. Communication theory of secrecy systems. *The Bell system technical journal*, 28(4):656–715, 1949.

[12] Ramona Wolf. Quantum key distribution. 2021.

[13] Charles H Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. *arXiv preprint arXiv:2003.06557*, 1984.

[14] Sheng-Kai Liao, Wen-Qi Cai, Wei-Yue Liu, Liang Zhang, Yang Li, Ji-Gang Ren, Juan Yin, Qi Shen, Yuan Cao, Zheng-Ping Li, et al. Satellite-to-ground quantum key distribution. *Nature*, 549(7670):43–47, 2017.

[15] Sebastian Ecker, Bo Liu, Johannes Handsteiner, Matthias Fink, Dominik Rauch, Fabian Steinlechner, Thomas Scheidl, Anton Zeilinger, and Rupert Ursin. Strategies for achieving high key rates in satellite-based qkd. *npj Quantum Information*, 7(1):5, 2021.

[16] Thomas Jennewein, Christoph Simon, Andre Fougeres, Francois Babin, Faezeh Kimiaee Asadi, Katanya B Kuntz, Mathieu Maisonneuve, Brian Moffat, Kimia Mohammadi, and Denis Panneton. Qeyssat 2.0–white paper on satellite-based quantum communication missions in canada. *arXiv preprint arXiv:2306.02481*, 2023.

[17] Hitoshi Inamori, Norbert Lütkenhaus, and Dominic Mayers. Unconditional security of practical quantum key distribution. *The European Physical Journal D*, 41:599–627, 2007.

[18] Stefano Pirandola, Ulrik L Andersen, Leonardo Banchi, Mario Berta, Darius Bunandar, Roger Colbeck, Dirk Englund, Tobias Gehring, Cosmo Lupo, Carlo Ottaviani, et al. Advances in quantum cryptography. *Advances in optics and photonics*, 12(4):1012–1236, 2020.

[19] European Space Agency. Types of orbits, 2020. Accessed: 2024-10-02.

[20] Jasminder S Sidhu, Thomas Brougham, Duncan McArthur, Roberto G Pousa, and Daniel KL Oi. Finite key performance of satellite quantum key distribution under practical constraints. *arXiv preprint arXiv:2301.13209*, 2023.

[21] Zhixiang Gao, Aijun Liu, and Xiaohu Liang. The performance analysis of downlink noma in leo satellite communication system. *IEEE access*, 8:93723–93732, 2020.

[22] Ramona Wolf. Security of Quantum Key Distribution 10: Eavesdropping Strategies, 2020.

[23] Larry C Andrews and Ronald L Phillips. Laser beam propagation through random media. *Laser Beam Propagation Through Random Media: Second Edition*, 2005.

[24] Hemani Kaushal, VK Jain, and Subrat Kar. *Free space optical communication*, volume 60. Springer, 2017.

[25] Mohammad Ali Khalighi and Murat Uysal. Survey on free space optical communication: A communication theory perspective. *IEEE communications surveys & tutorials*, 16(4):2231–2258, 2014.

[26] Franz Fidler, Markus Knapek, Joachim Horwath, and Walter R Leeb. Optical communications for high-altitude platforms. *IEEE Journal of selected topics in quantum electronics*, 16(5):1058–1070, 2010.

[27] Janusz Mikołajczyk, Zbigniew Bielecki, Maciej Bugajski, Józef Piotrowski, Jacek Wojtas, Waldemar Gawron, Dariusz Szabra, and Artur Prokopiuk. Analysis of free-space optics development. *Metrology and Measurement Systems*, 24(4):653–674, 2017.

[28] Alan Zucconi. Atmospheric scattering: The Rayleigh and Mie effects, 2017. Accessed: 2024-08-08.

[29] F Patat, OS Ugolnikov, and OV Postylyakov. Ubvri twilight sky brightness at eso-paranal. *Astronomy & Astrophysics*, 455(1):385–393, 2006.

[30] Mostafa Abasifard, Chanaprom Cholsuk, Roberto G Pousa, Anand Kumar, Ashkan Zand, Thomas Riel, Daniel KL Oi, and Tobias Vogl. The ideal wavelength for daylight free-space quantum key distribution. *arXiv preprint arXiv:2303.02106*, 2023.

[31] WN Peters and AM Ledger. Techniques for matching laser tem 00 mode to obscured circular aperture. *Applied Optics*, 9(6):1435–1442, 1970.

[32] Bernard J Klein and John J Degnan. Optical antenna gain. 1: Transmitting antennas. *Applied optics*, 13(9):2134–2141, 1974.

[33] Alan E Hedin. Extension of the msis thermosphere model into the middle and lower atmosphere. *Journal of Geophysical Research: Space Physics*, 96(A2):1159–1172, 1991.

[34] Alan E Hedin, MA Biondi, RG Burnside, G Hernandez, RM Johnson, TL Killeen, C Mazaudier, JW Meriwether, JE Salah, RJ Sica, et al. Revised global model of thermosphere winds using satellite and ground-based observations. *Journal of Geophysical Research: Space Physics*, 96(A5):7657–7688, 1991.

[35] John C Barentine. Night sky brightness measurement, quality assessment and monitoring. *Nature Astronomy*, 6(10):1120–1132, 2022.

[36] National Weather Service. Twilight types. `https://www.weather.gov/lmk/twilight-types`. Accessed: 2024-07-30.

[37] Paul Martini. Useful astronomical data, 2022. Accessed: April 25, 2024.

[38] Salvador Bará, Martin Aubé, John Barentine, and Jaime Zamorano. Magnitude to luminance conversions and visual brightness of the night sky. *Monthly Notices of the Royal Astronomical Society*, 493(2):2429–2437, 2020.

[39] Ferdinando Patat. Ubvri night sky brightness during sunspot maximum at eso-paranal. *Astronomy & Astrophysics*, 400(3):1183–1198, 2003.

[40] Fernando Patat. Inquiry regarding "ubvri twilight sky brightness at eso-paranal" for master thesis, 2024. Personal communication via email.

[41] Anthony Bucholtz. Rayleigh-scattering calculations for the terrestrial atmosphere. *Applied optics*, 34(15):2765–2773, 1995.

[42] Quanfu He, Zheng Fang, Ofir Shoshanim, Steven S Brown, and Yinon Rudich. Scattering and absorption cross sections of atmospheric gases in the ultraviolet–visible wavelength range (307–725 nm). *Atmospheric Chemistry and Physics*, 21(19):14927–14940, 2021.

[43] Ryan Thalman, Kyle J Zarzana, Margaret A Tolbert, and Rainer Volkamer. Rayleigh scattering cross-section measurements of nitrogen, argon, oxygen and air. *Journal of Quantitative Spectroscopy and Radiative Transfer*, 147:171–177, 2014.

[44] Andrew T Young. On the rayleigh-scattering optical depth of the atmosphere. *Journal of Applied Meteorology (1962-1982)*, pages 328–330, 1981.

[45] Barry A Bodhaine, Norman B Wood, Ellsworth G Dutton, and James R Slusser. On rayleigh optical depth calculations. *Journal of Atmospheric and Oceanic Technology*, 16(11):1854–1861, 1999.

[46] F Patat, S Moehler, K O'Brien, E Pompei, Thomas Bensby, Giovanni Carraro, A de Ugarte Postigo, A Fox, I Gavignaud, G James, et al. Optical atmospheric extinction over cerro paranal. *Astronomy & Astrophysics*, 527:A91, 2011.

[47] Earl J McCartney. Optics of the atmosphere: scattering by molecules and particles. *New York*, 1976.

[48] Kuo-Nan Liou. *An introduction to atmospheric radiation*, volume 84. Elsevier, 2002.

[49] Kevin Krisciunas and Bradley E Schaefer. A model of the brightness of moonlight. *Publications of the Astronomical Society of the Pacific*, 103(667):1033, 1991.

[50] Wikipedia contributors. Surface brightness — Wikipedia, the free encyclopedia. `https://en.wikipedia.org/wiki/Surface_brightness`, 2023. Accessed: 16-October-2024.

[51] Andrew Crumey. Human contrast threshold and astronomical visibility. *Monthly Notices of the Royal Astronomical Society*, 442(3):2600–2619, 2014.

[52] Xiongfeng Ma, Bing Qi, Yi Zhao, and Hoi-Kwong Lo. Practical decoy state for quantum key distribution. *Physical Review A*, 72(1):012326, 2005.

[53] Xiang-Bin Wang. Decoy-state protocol for quantum cryptography with four different intensities of coherent light. *Physical Review A*, 72(1):012322, 2005.

[54] Manuel Erhard. Personal communication. Conversation, April 2024.

[55] Wolfgang Demtröder. *Experimentalphysik 3: Atome, Moleküle und Festkörper*. Springer-Verlag, 2016.

[56] Bureau of Meteorology Space Weather Services. The luminosity of the sun, Datum, wann die Seite besucht wurde. 2024-03-04.

[57] Maarten Sneep and Wim Ubachs. Direct measurement of the rayleigh scattering cross section in various gases. *Journal of Quantitative Spectroscopy and Radiative Transfer*, 92(3):293–310, 2005.

[58] Edgar Woolard. *Spherical astronomy*. Elsevier, 2012.

[59] Marcus Huber and Friis. Lecture notes: Quantum channels. *TU VIENNA*, 16(4):2231–2258, 2022.

[60] Stephane Attal. Quantum channels. *Institut Camille Jordan, University of Lyon*, 2014.

[61] Larry C Andrews and Ronald L Phillips. Laser beam propagation through random media. *Laser Beam Propagation Through Random Media: Second Edition*, 2005.

[62] Xiaoming Zhu and Joseph M Kahn. Free-space optical communication through atmospheric turbulence channels. *IEEE Transactions on communications*, 50(8):1293–1300, 2002.

[63] Kerry A Mudge, KKMB Dilusha Silva, Bradley A Clare, Kenneth J Grant, and Brett D Nener. Scintillation index of the free space optical channel: Phase screen modelling and experimental results. In *2011 International Conference on Space Optical Systems and Applications (ICSOS)*, pages 403–409. IEEE, 2011.

[64] Xiaoming Zhu and Joseph M Kahn. Free-space optical communication through atmospheric turbulence channels. *IEEE Transactions on communications*, 50(8):1293–1300, 2002.

[65] Sheng-Kai Liao, Hai-Lin Yong, Chang Liu, Guo-Liang Shentu, Dong-Dong Li, Jin Lin, Hui Dai, Shuang-Qiang Zhao, Bo Li, Jian-Yu Guan, et al. Long-distance free-space quantum key distribution in daylight towards inter-satellite communication. *Nature Photonics*, 11(8):509–513, 2017.

[66] Veronica Fernandez, Jorge Gómez-García, Alejandro Ocampos-Guillén, and Alberto Carrasco-Casado. Correction of wavefront tilt caused by atmospheric turbulence using quadrant detectors for enabling fast free-space quantum communications in daylight. *IEEE Access*, 6:3336–3345, 2018.

[67] Andrej Krzic, Daniel Heinig, Matthias Goy, and Fabian Steinlechner. Dual-downlink quantum key distribution with entangled photons: prospects for daylight operation. In *International Conference on Space Optics—ICSO 2022*, volume 12777, pages 909–924. SPIE, 2023.

[68] W Forrest Stinespring. Positive functions on *-algebras. *Proceedings of the American Mathematical Society*, 6(2):211–216, 1955.

[69] Debbie Leung and John Watrous. On the complementary quantum capacity of the depolarizing channel. *Quantum*, 1:28, 2017.

[70] Charles H Bennett, David P DiVincenzo, and John A Smolin. Capacities of quantum erasure channels. *Physical Review Letters*, 78(16):3217, 1997.

[71] Masahito Hayashi. *Quantum information theory*. Springer, 2016.

[72] Charles H Bennett, Gilles Brassard, and N David Mermin. Quantum cryptography without bell's theorem. *Physical review letters*, 68(5):557, 1992.

[73] Artur K Ekert. Quantum cryptography based on bell's theorem. *Physical review letters*, 67(6):661, 1991.

[74] Ronald L Rivest, Adi Shamir, and Leonard Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.

[75] Alessia Scriminich, Giulio Foletto, Francesco Picciariello, Andrea Stanco, Giuseppe Vallone, Paolo Villoresi, and Francesco Vedovato. Optimal design and performance evaluation of free-space quantum key distribution systems. *Quantum Science and Technology*, 7(4):045029, 2022.

[76] William K Marshall. Transmitter pointing loss calculation for free-space optical communications link analyses. *Applied optics*, 26(11):2055_1–2057, 1987.

[77] Tobias Schmitt-Manderbach, Henning Weier, Martin Fürst, Rupert Ursin, Felix Tiefenbacher, Thomas Scheidl, Josep Perdigues, Zoran Sodnik, Christian Kurtsiefer, John G Rarity, et al. Experimental demonstration of free-space decoy-state quantum key distribution over 144 km. *Physical Review Letters*, 98(1):010504, 2007.