Quantum Key Distribution through atmospheric turbulence : secure satellite-to-ground links

Valentina Marulanda Acosta

Quantum Key Distribution through atmospheric turbulence: secure satellite-to-ground links

Valentina Marulanda Acosta
HRA-ONERA et QI-LIP6 Sorbonne Université

Thèse de Doctorat de Sorbonne Université. Ecole Doctorale Informatique, Télécommunications et Electronique

Présentée et soutenue publiquement le 4 décembre 2023, devant un jury composé de :

Eleni Diamanti
Directrice de thèse, DR, CNRS,
Sorbonne Université, France.

Caroline B. Lim
Encadrante, Ingénieure de recherche,
LNE-SYRTE, Observatoire de Paris

Jean-Marc Conan
Encadrant, Ingénieur de recherche,
DOTA, ONERA, Université Paris Saclay

Daniele Dequal
Invité,
ESTEC, Noordwijk, Pays-Bas

Giuseppe Vallone
Rapporteur, Professeur,
Université de Padova, Padoue, Italie

Thomas Jennewein
Rapporteur, Professeur,
IQC, Waterloo, Canada

Ghaya Rekaya
Examinatrice, Professeure,
Telecom Paris

Andrew Thain
Examinateur,
ADS Toulouse

Résumé

Les exigences sans cesse croissantes des systèmes de télécommunication modernes en termes de débit, ainsi que la menace imminente que pose l'augmentation de la puissance de calcul des ordinateurs modernes sur les méthodes cryptographiques actuelles, font de la transmission sécurisée des données à la fois une exigence essentielle et un grand défi, et donc un domaine d'étude très actif. La distribution quantique des clés (QKD) permet l'échange de clés cryptographiques dont le niveau de sécurité ne dépend pas de la complexité d'un algorithme mathématique mais repose intrinsèquement sur l'exploitation des propriétés de la mécanique quantique.

Cependant, le déploiement des systèmes QKD via des réseaux fibrés terrestres, est fortement limité en distance, et n'atteint que quelques centaines de kilomètres, en raison de l'atténuation exponentielle subie par les signaux transmis par fibre optique. Les méthodes d'amplification des répéteurs de communications optiques classiques ne sont pas compatibles avec un signal quantique, et en raison du manque de maturité technologique concernant les répéteurs quantiques, les relais satellite se présentent comme une alternative intéressante pour l'établissement de liaisons quantiques intercontinentales sécurisées.

Nous présentons ici, dans le contexte d'un lien QKD descendant entre un satellite en orbite basse et le sol, un modèle complet du canal atmosphérique satellite-sol prenant conjointement en compte la turbulence, sa correction partielle par optique adaptative (OA) les pertes géométriques et les fluctuations de pointage à bord du satellite. Nous utilisons ce modèle pour évaluer les performances de trois protocoles QKD - à variables continues et à variables discrètes, avec des photons uniques ou intriqués - pour différentes conditions de turbulence, différents degrés de correction par OA, différents scénarios de configuration du lien (diamètre télescope, altitude du satellite...) et en prenant en compte les effets de taille finie.

Les résultats obtenus montrent l'intérêt de l'utilisation d'un système d'OA : en effet , la performance en termes de taux de génération de clé de tous les protocoles analysés s'améliore en considérant une correction par OA. Cette augmentation du taux de clé est particulièrement significative pour les scénarios de forte turbulence, d'opération diurne et pour le protocole QKD à variables continues (CV). L'apport de l'OA est de plus démontré et quantifié dans une configuration très prometteuse exploitant l'émission de

deux photons intriqués vers deux stations sol depuis un relais satellite qui n'est pas forcément de confiance. Afin de valider nos résultats de simulation, nous avons aussi commencé à implémenter un banc de test expérimental à partir d'une émulation simplifiée du canal atmosphérique et d'un système CV-QKD. Nous expliquons les difficultés rencontrées pendant cette mise en œuvre ainsi que les solutions proposées et des idées sur les perspectives de l'étude.

Acknowledgements

The work presented in this manuscript was only possible thanks to the help and support of an entire army of people.

First and foremost I would like to thank my PhD supervisors Caroline, Eleni and Jean-Marc. I will forever be grateful to you for putting your trust in me and allowing me to embark in one of the most enriching and challenging adventures of my life. Your guidance and scientific expertise was fundamental to the evolution of the project but your humanity and kindness was immensely more invaluable to me.

To the members of the jury: Ghaya Rekaya, Thomas Jennewein, Giuseppe Vallone and Andrew Thain, thank you for having accepted to be part of my defense and for putting in the time and effort to both read about and listen to my work.

I would also like to thank Daniele Dequal for all the work done in our joint studies. Our scientific discussions and regular meetings were greatly appreciated. Big thanks to Matteo Schiavon, the most frequent victim of my constant questions who always found some time to answer.

Thanks to the adaptive optics team in Padova, Stefano Bonora, Antonio Vanzo and Kevin Campaci for welcoming me and letting me get some hands-on experience on turbulence correction systems.

Words are not enough to express the level of gratitude I have towards the HRA team at ONERA and the QI team at LIP6. The day-to-day struggles of doing a PhD were massively alleviated by being surrounded by such amazing people. From tarot, crossword puzzles and bubble tea to Hanabi, group retreats and Friday beers, I will forever cherish the time I got to spend with you all both inside and outside the labs.

I would like to thank the people at ONERA next to whom I started this crazy journey and whose support was essential to getting this show started, Alix with your incredible support, Perrine with your contagious joy, Pablo and Emile, all of whom I am confident will have brilliant futures ahead. Thanks to Laurie for being so caring and kind. Thanks as well to the more recent recruits and former PhDs, however limited my time with you was, I enjoyed and learned from every minute spent together.

Huge thanks to the QI team for helping me flourish personally and professionally in such a nurturing environment. The excitement and genuine curiosity regarding science from all members of the team kept me motivated through the latter half of my PhD. Thanks to Verena for your friendship and your support, I greatly appreciate your unapologetic and unique personality, you will be a legendary researcher, and you'll get your lab at Annecy (cuties included). Thanks to Laura for the always engaging conversations, judging of the French language, and multiple outside the lab activities. Thanks to Matilde for your endless energy and contagious enthusiasm. Thanks to Uta for the encouraging post-its, to Santiago for being my Spanish-speaking desk mate and pal, to Pascal for welcoming us in your home, to Paul for your kind demeanor and professional french-ness. Thanks to Adriano for your out-of-pocket comments and perennial tardiness, to Nicolas LP for your reluctant faith in me, to Dominik for the good vibes. Thanks to Yao for making the 4th of December twice as legendary. Thanks to Paolo, the most gastronomically open-minded Italian for your interest in satellite comms.

My deepest thanks to Yoann for your endless patience and constant encouragement. Writing a thesis is no easy feat and your presence was a major reason I kept pushing through. Thank you for your professional help inside the lab as well as your support on a personal level outside of it. The field of quantum communications is lucky to have such a talented researcher in its ranks, but I am even luckier for getting to have you in my life.

Thanks in no particular order to Luís, Hela, George, Léa, Michael, Kim, Ivan, Majid, Gizem, Damian, Alex, Fred, Hiyam, Mehdi, Yann, Yann LT, Timothée, Daniel, Aurélie, Mario, Paul H. This is far from being an exhaustive list, the amount of people who have left their mark on me during this journey is huge, I wish nothing but the best for you all and I will miss you dearly (even if I'm not going far).

Por último pero no menos importante, infinito agradecimiento a mi familia y amigos. A Laura que después de dos décadas aún no se ha cansado de mi, gracias por el apoyo incondicional y por estar siempre ahí. A Oscar que ha decidido embarcarse en esta misma travesía, ánimo, no es fácil pero vale la pena. Gracias también a Sebastián por todo su apoyo. Todos ustedes son mi familia lejos de la familia. Un agradecimiento inmenso para mi familia, mi mamá, mi tía y Susis, tres mujeres guerreras a las que les debo todo lo que soy. A Giova por su apoyo a lo largo de los años, y a las tres chifladas, Isabella, Gabriela y Mariana que son mi motivo más grande para salir adelante.

Contents

Introduction

The ever-growing demands of modern telecommunication systems in terms of data rates as well as the impending threat of the increasing computing power of modern computers, make the secure transmission of data an essential requirement and thus a very active field of study. Quantum key distribution (QKD) allows for the exchange of cryptographic keys whose security level does not depend on the complexity of a mathematical algorithm but instead relies intrinsically on exploiting the properties of quantum mechanics [1]. Depending on the protocol, the key bits will be encoded either on the superposition of modes of individual photons, such as polarization modes, as is the case for the discrete variable protocols (DV) or they will be encoded into the quadratures of a very low flux electromagnetic field as it happens in the continuous variable protocols (CV).

While offering security levels unattainable by classical means, QKD protocols in their terrestrial implementation are severely limited in distance reaching only several hundred kilometers because of the exponential attenuation suffered by fiber-transmitted signals. Since the amplification methods of classical optical communications repeaters are not compatible with a signal that is quantum in nature, and because of the current lack of technological maturity regarding quantum repeaters, satellite relays present an interesting alternative for the establishment of secure intercontinental quantum links [2].

A study by Dequal et al. [3] upon which a part of the present study is based on, examines the possibility of performing a continuous variable key exchange between a satellite and a ground station by proposing a modeling of the propagation channel accounting for the effects of beam wandering, a fluctuating atmospheric transmission and a fixed loss due to the turbulence effects on single mode fiber coupling.

We have chosen to estimate the impact of atmospheric turbulence on coupling in the fiber using a more detailed model. In particular, we add the effects of propagation on the spatial coherence of the optical signal. Adaptive optics (AO) can partially correct the propagation effects mentioned above. A typical AO system consists of a feedback loop containing elements capable of measure and correct wavefront aberrations in real time. In this study, we focus our efforts on analyzing the influence of such a system on the performance of several QKD protocols in different scenarios.

This is done by taking into account several variables that affect the optical signal as it propagates through the atmosphere. The impact of geometric losses, beam wandering, light absorption and scattering, as well as wavefront aberrations and their partial correction by adaptive optics are among the parameters we modelled and simulated. These simulations are combined to obtain a statistical description of the channel's transmission efficiency. Based on this representation, we examine the performance of three QKD protocols by calculating their key generation rates for a range of turbulence conditions and considering correction schemes of different levels of complexity.

Manuscript outline

This manuscript details the process of modelling, simulation and performance analysis of quantum key distribution satellite-to-ground links.

Chapter 1 contains the theoretical explanation of quantum key distribution. It introduces relevant concepts related to cryptography and quantum mechanics as well as the general operating principle and motivation behind quantum key distribution. Afterwards we present the two main families of protocols, discrete variable and continuous variable, and we summarize their differences as well as give a general description of three specific protocols. For each protocol presented, we provide an explanation of the stages involved in its execution as well as the analytical formulas related to the secret key rate computation.

Chapter 2 introduces propagation of an optical wave through an atmospheric channel. Here we explain how we have decided to model turbulence effects and the impact they have on the optical wavefront, particularly on the coupling into a single mode fiber. We then present the general concept behind a turbulence mitigation approach called adaptive optics. Next we present a pseudo-analytic simulation tool designed at ONERA that estimates the behavior of fiber coupling under certain turbulence conditions. Finally, we introduce some additional atmospheric effects such as path loss, beam wandering and absorption in order to account for the most important contributing factors to the loss of a satellite-to-ground optical channel.

Chapter 3 includes our first full simulation study, featuring quantum key distribution over a single satellite-to-ground link aided by adaptive optics. We present the specifics of the scenario considered as well as the reference values of multiple parameters and their justification. We explain the simulation process and delve into the details of each step of the process, including the construction of altitude dependent turbulence profiles, fiber coupling efficiency estimations and computation of path loss and beam wandering effects. Then, we detail the method employed to integrate the aforementioned intermediary results in order to obtain a complete statistical representation of the transmission efficiency of the atmospheric channel. Said probabilistic description

allows us to finally calculate the final performance metric of such a system, the secret key rate. This is done for a continuous variable (CV) and a discrete variable (DV) prepare and measure protocol.

Chapter 4 contains the results of our second simulation study. Here we expand upon the performance evaluation of a satellite-to-ground quantum link by analyzing a scenario involving an entangled photon quantum key distribution protocol with the satellite as an untrusted node. In order to do this, we explain the estimation of the transmission efficiency of two different atmospheric channels, corresponding to two different ground station locations. Similarly to the first study we present our simulation methodology and examine the resulting performance of the entangled protocol via the computation of the secret key rate.

Chapter 5 includes the preliminary results aiming at the development of an experimental validation of our simulation results. The first approach involves a channel emulator capable of reproducing the losses of the atmospheric link, coupled with a continuous variable quantum key distribution experimental bench already existing at LIP6. The second approach involves some in-lab and field tests of an alternative correction scheme involving a tunable prism or a deformable lens done in collaboration with the CNR-IFN in Padova. In this chapter we discuss the difficulties encountered during the different experimental attempts and some potential solutions, as well as further perspectives for the continuation of the work presented in this thesis.

Chapter 6 ends by providing a synthesis of the main results of this thesis, as well as the conclusions reached throughout the present work. We also briefly discuss some unsolved challenges and further perspectives on ways that future efforts could expand upon our analysis.

Publications

The results from chapter 3 have been submitted for publication in the following manuscript:

- [4] *Analysis of satellite-to-ground quantum key distribution with adaptive optics*, with D. Dequal, M. Schiavon, A. Montmerle-Bonnefois, C.B. Lim, JM. Conan and E. Diamanti.

The results from chapter 4 will soon be submitted for publication in the following manuscript (currently in preparation):

- *Increasing the secret key rate of satellite-to-ground entanglement-based QKD assisted by adaptive optics*, with D. Dequal, M. Schiavon, A. Montmerle-Bonnefois, C.B. Lim, JM. Conan and E. Diamanti.

An additional a contribution was made regarding a simplified satellite-to-ground channel model in the following manuscript, which will soon be submitted for publication:

- [5] *Connecting Quantum Cities: Simulation of a Satellite-Based Quantum Network*, with R. Yehia, M. Schiavon, T. Coopmans, I. Kerenidis, D. Elkouss and E. Diamanti.

The results of this thesis were also presented as posters in conferences such as IQFA 2021 and 2022, QCMC 2022 and QCRYPT 2022, as well as through oral presentations at JRIOA-SFO 2021 and OFC 2023.

Chapter 1

Quantum Key Distribution

Quantum key distribution (QKD) is the name given to a diverse set of protocols that exploit the properties of quantum mechanics in order to exchange *information-theoretic* secure cryptographic keys. In this section, we will give a brief introduction to pertinent cryptography concepts, and quantum mechanics concepts relevant to key distribution, as well as the motivation for and general explanation of QKD.

We will then look more in depth into the two main families of QKD protocols, continuous variable (CV) and discrete variable (DV), and we will explain the principle behind three specific QKD protocols: two DV protocols (two-decoy efficient BB84 and BBM92) and one CV protocol (GG02). We will see as well the specifics of the secret key rate (SKR) calculations for all the aforementioned protocols in both the asymptotic and the finite-size regimes.

1.1 Introduction

Cryptography is a branch of science at the intersection of the fields of mathematics and information theory. It is a set of well known techniques that have for a very long time been used in order to secure communication channels. The rise of quantum computers, is however threatening the security of classical cryptographic protocols; hence it is important to look into how certain quantum properties could be utilized to enhance security at a fundamental level.

1.1.1 Introduction to cryptography

The basic principle of cryptography is to hide a message in such a way that only the entities for which it is meant can understand it. In a general description, Alice and Bob share a communication channel through which they wish to exchange information, however they want it to only be accessible by them and not be intercepted by a third party often called eavesdropper or Eve.

One way they can hide the original message is to transform it through some kind of encryption function or algorithm. Bob has a message m and wants to covertly send it to Alice, he thus applies encryption function E such that a secret message $m_s = E(m)$ is obtained and transmitted. Alice then needs to decipher the original message with a decryption function D that reverses the effects of E such that $D(m_s) = m$.

Asymmetric encryption

When Bob's encryption *key* is public and available to the eavesdropper (as well as any other party wishing to communicate with him), while his decryption key is private and thus only known by himself we have what is called *public key encryption* or *asymmetric encryption*. Within this scheme both Alice and Bob can each have a public key and a private key rendering communication bidirectional. Such a setup can also be employed for digital signatures, Alice (indirectly) uses her private key as a signature so that any message she sends can be verified to be sent by her. Bob can check this via the public key and no user in the system could forge that signature without knowledge of Alice's private key.

A prime example of public key encryption is the RSA algorithm [6]. This protocol proposed for the British intelligence agency in 1973 and later declassified in 1977, is currently very widely spread in secure data transmission systems. The security of this specific algorithm relies on the practical difficulty of factoring large prime numbers. Here, the public key n consists of the product of two very large prime numbers p and q while the private key d is a number that's relatively prime to $(p-1)(q-1)$.

When the user has knowledge of the private key, decrypting the message (i.e. finding p and q) is a relatively easy operation. However, without it, factoring of the private key is necessary which is computationally a very costly process. Even the best classical factoring algorithm currently known, the general number field sieve (GNFS) [7] would take over a billion years to factor a public RSA key of only 2048 digit length.

Symmetric encryption

In contrast, when both Alice and Bob share the same secret private key, we have what is called *private key encryption* or *symmetric encryption*. A simple example of a symmetric encryption algorithm is the one-time pad. Here, the key is a secret random string of bits known exclusively by Alice and Bob, it's of the same length as the message to be exchanged, and it must be used only once in order to achieve perfect secrecy. In a simple example, each key bit can for instance determine whether the corresponding message bit has been flipped (if key bit = 1) or not (if key bit = 0) [8]. The clear problem of this specific algorithm is the length of the single-use key which while it makes the algorithm secure, translates into very high memory use and a slow performance. A more complex and widely spread algorithm is the AES or advanced encryption standard. It encrypts blocks of information by performing a series of linked substitution and permutation operations on the message, with the operations being determined by the secret key [9].

Regardless of the encryption algorithm, symmetric protocols have one crucial issue: their security relies on the secrecy of the key shared between Alice and Bob. The problem becomes apparent in the process of distributing or sharing that key in such a way that it is kept secret from eavesdroppers. Asymmetric algorithms tend to be slower and require longer keys while symmetric ones are often faster and deal better with encoding information in bulk. Therefore, in practice, asymmetric-key encryption is often used to exchange the keys necessary for symmetric-key encryption.

It is important to note that both the RSA and AES protocols, upon which a considerable amount of information security is currently based, are computationally secure. That means that while in theory the private keys could be mathematically computed (by brute force or otherwise), the computational cost of such process in terms of number of operations is so high that in practice, it is believed that no classical computer would be able to break a long enough encryption key.

Shor and Grover algorithms

The existence of quantum computers is nevertheless threatening the security of classical encryption schemes. Research on and development of quantum computers is currently a very active field advancing relentlessly. Multiple quantum algorithms have been proposed, but two are of particular interest to us: Shor's algorithm and Grover's algorithm.

Shor's algorithm, proposed in 1994 [10] when performed by a quantum computer would allow for the factorization of large numbers significantly faster than any known classical algorithm. For comparison, the number of operations needed for the GNFS algorithm is sub-exponential but super-polynomial with the length of the number while for Shor's algorithm it is polynomial with the logarithm of the length of the number [7, 10]. Attacks of the type *store-now-attack-later*, pose a problem for the security of public key algorithms such as the RSA. When a quantum computer with a large enough amount of qubits and noise tolerance is built, the security of these algorithms will be jeopardized to a greater extent.

Grover's algorithm, is a quantum algorithm proposed in 1996 [11] that when performed by a quantum computer can find (with high probability) the input of an unknown function given the output of the function. Similarly to Shor's algorithm, Grover's would allow a considerable speed up in comparison to the best classical strategies, although not exponential in this case. Classically, figuring out the input would require an amount of operations linear with the length of the input, while with this quantum algorithm it would be proportional to the square root of the length of the input.

We can see that Shor's algorithm will in time be able to break asymmetric encryption algorithms like the RSA, while Grover's algorithm could provide a significant advantage for cracking symmetric encryption algorithms like the AES. Moreover, multiple other

algorithms that may threaten the security of modern encryption schemes could still be developed in the future. Two schools of thought have surged upon this problem, on one hand research into classical algorithms capable to withstand quantum attacks is being done; this field is called *post-quantum cryptography*. On the other hand, research is being conducted into developing new cryptographic strategies, more particularly key distribution protocols, that employ the properties of quantum mechanics in order to guarantee security levels that are more than computationally-secure, that is, not dependent on the computational power of the adversary. It is this latter field of research, called *quantum key distribution* (or QKD) the one we will be focusing on going forward.

1.1.2 Relevant quantum principles

Before getting into the intricacies of the different QKD protocols, we will first introduce the different properties of quantum mechanics that give these types of protocols security levels unattainable by classical means.

Quantum state representation

We can start the description of quantum mechanical systems by the definition of their states, usually described as vectors of a Hilbert space $\mathcal{H}$. The simplest kind of quantum system, a qubit, has two possible states $|0\rangle$ and $|1\rangle$, corresponding to the vectors:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{1.1.1}$$

Any qubit can thus be represented as a superposition of these two states as such:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \tag{1.1.2}$$

Here $|\alpha|^2$ and $|\beta|^2$ represent the probability of the system to be measured in each of the respective states with $|\alpha|^2 + |\beta|^2 = 1$. Qubits are the basic element of what is called *discrete variable* quantum communication since the quantum states used to encode the information live in a finite dimension Hilbert space. In our case, we specifically consider the polarization of photons as our chosen way to implement qubits [12]. Photons are primarily used in quantum communications due to their low decoherence and the fact that means of transporting them, e.g. optical fiber, are already widely available.

Another family of quantum communication protocols also exists, the so-called *continuous variable* protocols. Instead of relying on conveying information through discrete degrees of freedom of individual particles, continuous state protocols employ weak coherent pulses of light and encode information into the quadratures of its electromagnetic field. Coherent states can also be expressed as a superposition of states, in this case a

superposition of photon number states $|n\rangle$ such as:

$$|\alpha\rangle = e^{\frac{-|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle \tag{1.1.3}$$

This type of states, also called quasi-classical states, will have n number of photons with probability $P(n) = e^{-|\alpha|^2} \frac{\alpha^{2n}}{n!}$. The mean value of photons of coherent state $|\alpha\rangle$ will then be $|\alpha|^2$.

Both coherent states and qubits follow the rules of quantum mechanics and are bound by certain theorems and physical laws that differ from their classical counterparts. In the following, we will analyze those most significant to explain the relevance of the QKD protocols we have chosen to study.

No-cloning theorem

Originally demonstrated in 1982, the no-cloning theorem states that a device capable of perfectly replicating any unknown quantum state cannot exist [13]. A simple way to prove this is as follows; we can model the hypothetical cloning device as a unitary operator U taking qubit $|\psi\rangle$ and copying it into a second, vacuum qubit $|0\rangle$ as such:

$$\begin{aligned} U[|\psi\rangle|0\rangle] &= |\psi\rangle|\psi\rangle \\ &= (\alpha|0\rangle + \beta|1\rangle)(\alpha|0\rangle + \beta|1\rangle) \\ &= \alpha^2|0\rangle|0\rangle + \alpha\beta|0\rangle|1\rangle + \beta\alpha|1\rangle|0\rangle + \beta^2|1\rangle|1\rangle \end{aligned} \tag{1.1.4}$$

However, since quantum theory is linear, the cloning operator should act on state $|\psi\rangle$ (defined by equation 1.1.2) as described below.

$$U[(\alpha|0\rangle + \beta|1\rangle)|0\rangle] = \alpha U[|0\rangle|0\rangle] + \beta U[|1\rangle|0\rangle] = \alpha|0\rangle|0\rangle + \beta|1\rangle|1\rangle \tag{1.1.5}$$

Since the results in equations 1.1.4 and 1.1.5 should both be valid, yet they end up contradicting each other, we can deduce that a cloning device U cannot be possible. Within the context of secure communication this means that any quantum state sent by Alice to Bob cannot be intercepted and copied by Eve without her interference being detected.

Entanglement

Entanglement is a property unique to quantum systems in which the correlations between two spatially separated parts of a state, cannot be described locally by classical means [14].

In the early to mid 20th century, physicists looked for a way to explain the correlations between spatially separated particles. In 1935 Einstein, Podolsky and Rosen

proposed a description based on the idea that hidden local variables were shared between the particles before they were separated [15]. Later on, in 1964, Bell proposed a mathematical description of the inequalities that a system described following this EPR model would need to fulfill [16]. Since then, starting in 1972 [17] multiple experimental demonstrations have been performed that show a violation of the inequalities proposed by Bell, proving that EPR local realism was not enough to describe certain particle correlations.

Let us consider that Alice and Bob share a two-qubit quantum state $|\phi\rangle$, where qubit A is at Alice's location and qubit B is at Bob's. If we can express $|\phi\rangle$ as the product of Alice's and Bob's states, it corresponds to a separable state. If we take $|\phi\rangle = |0_A\rangle|0_B\rangle$ for example, it is clear that Alice and Bob can determine the state of their own qubit independently of one another. In contrast, a quantum state like the one described by equation 1.1.6, cannot be separated into a product and is thus said to be *entangled*.

$$|\psi\rangle_{AB} = \frac{|0_A\rangle|0_B\rangle + |1_A\rangle|1_B\rangle}{\sqrt{2}} \tag{1.1.6}$$

In this case, $|\psi\rangle_{AB}$ is a superposition of two separable states. The status of Alice's qubit is intrinsically linked to Bob's, knowledge of the individual states each party holds cannot be assessed separately. Such states exhibit *non-local* correlations, that is, their measurement statistics cannot be described by local realism.

Heisenberg uncertainty

Heisenberg's uncertainty principle first postulated in 1927 [18], explains that in quantum mechanics there is a fundamental limit to the accuracy with which two conjugate variables can be determined. The complementary pair of variables that are of particular interest for our protocols are the quadratures of the electromagnetic field as shown below:

$$\Delta X \Delta P \geq \frac{\hbar}{2} \tag{1.1.7}$$

This means that it will not be possible to measure both of the quadratures perfectly precisely and the $\hbar/2$ limit that we will call 1 Shot Noise Unit (SNU) denotes the minimal noise our coherent or quasi-classical states will have.

1.1.3 QKD

Quantum Key Distribution is a family of protocols proposed in order to exchange keys between two parties in such a way that the security achieved is higher than the one obtained with classical cryptographic protocols. In particular, QKD protocols that we will discuss in more detail later on, exploit one or more of the fundamental quantum properties explained above in order to make the security of the key exchange

information-theoretic.

Information-theoretic security means the system is secure against an adversary possessing unlimited computing time and resources. This is because instead of relying on mathematical properties and the fact that it would be too computationally costly to break them (as is the case for classical protocols), quantum cryptographic protocols rely on the fact that the fundamental laws of quantum mechanics dictate that any intervention by an eavesdropper *will* be detected, and therefore no key will be exchanged when Eve has knowledge on it.

A generic QKD protocol setup is portrayed in figure 1.1. Alice and Bob, the two trusted parties wishing to secure their information, share two channels: a unidirectional quantum channel and a bidirectional authenticated classical channel they use for error correction and privacy amplification, which are respectively processes that they employ in order to guarantee the final shared key is identical and secure. Each one of them has an enclosed lab in a secure physical location, containing the optical components necessary for transmission and(or) reception in both of the channels, and the computer equipment required to perform digital signal processing, error correction, etc. Alice and Bob's devices such as the random generators, the detectors and sources are considered to be trusted. A third party called Eve, will try to eavesdrop into Alice & Bob's exchanges. We assume that Eve is able to read the classical channel and can read and write in the quantum channel. In addition to that she has her own lab, and we even consider she has access to a quantum computer, quantum memories and any hardware that is bounded by the laws of physics.

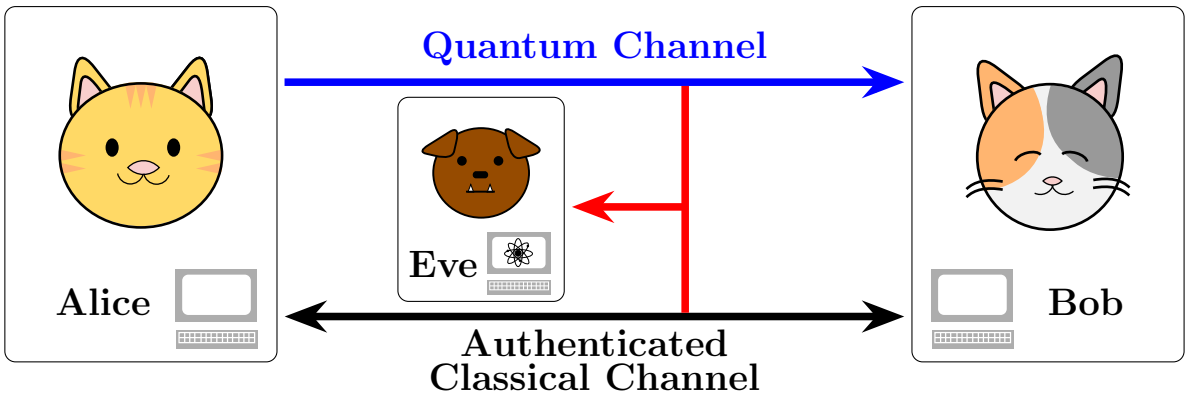


Figure 1.1: Generic schema of a quantum key distribution protocol

The basic procedure in what is called a *Prepare and Peasure* (PM) QKD protocol is as follows: Alice prepares a series of randomly generated quantum states in which the bits of the future key are encoded. The states go through the quantum channel where

they interact with the environment and a potential eavesdropper, arriving at Bob's lab with some amount of noise. Bob proceeds to measure the states and through a series of back and forth communication through the classical channel with Alice (the specifics of which depend on the specific protocol), they estimate the errors in the quantum information exchange. Depending on the protocol, either all errors or all noise beyond a baseline value are attributed to Eve.

After determining the errors of their quantum information exchange, Alice and Bob can proceed to correct them and apply a privacy amplification protocol to make Eve's information about the final key negligible. By the end of the classical reconciliation process, after making sure the string of key bits they now both possess is identical and secret, they can employ it in order to encrypt their messages exchanges via a symmetric encryption algorithm. The latter could be for example the one time pad (OTP) protocol since it is information-theoretical secure.

1.2 Discrete variable QKD

The first family of protocols we will look into is the discrete variable quantum key distribution (DV-QKD). These types of schemes encode the information of the key in the superposition of modes of single photons, in our case, we assume it to be encoded into the polarization [19] of the photons but schemes with encoding in phase, temporal modes or orbital angular momentum also exist. We will examine two protocols in detail, BB84 based on the transmission and encoding of individual photons and BBM92 which relies on entangled photon pairs.

1.2.1 BB84 protocol

The first QKD protocol was proposed by Bennett and Brassard in 1984 [20]. The information of the key is encoded in one of two non-orthogonal polarization bases, basis Z consisting of the states $|H\rangle = |0\rangle$ and $|V\rangle = |1\rangle$, or basis X consisting of the states $|D\rangle = \frac{|H\rangle+|V\rangle}{\sqrt{2}}$ and $|A\rangle = \frac{|H\rangle-|V\rangle}{\sqrt{2}}$. The protocol is depicted in figure 1.2 and can be described as follows:

1) Alice generates a random series of bits to be encoded into the photons.

2) For each bit, she randomly chooses one of the bases, she emits a polarized photon correspondingly, and then she sends it to Bob. For example if Alice's bit is 0, and she choses the Z basis, she sends a photon in the $|0\rangle = |H\rangle$ state, if the bit is 1, she polarizes it with the $|1\rangle = |V\rangle$ state.

3) Bob then receives the polarized photon and chooses at random (and independently for each qubit) one of the two bases to measure it. If he measures the bit in the

same basis Alice has encoded it and there were no errors, he correctly determines whether Alice sent a 0 or a 1. However, if he chooses the wrong basis the resulting bit has a 50% chance of coinciding with the one Alice sent. Measuring the qubits sent by Alice will leave Bob with a string of bits called the *raw key*.

4) Due to the random choice of measurement basis, Bob's raw key and the information Alice sent are only partially correlated. In order to obtain a fully correlated set of bits, Bob now reveals to Alice the basis he used to measure each of the qubits via the classical channel.

5) Alice compares Bob's bases with the ones she used to encode the bits, and she announces which ones he chose correctly. Both Alice and Bob only keep the bits for which the bases used for encoding and decoding were the same, discarding the rest. This now reduced bit sequence is called the *sifted key*.

6) Alice and Bob then share a random portion of their sifted keys, they compare it bit by bit and determine an estimation of the Quantum Bit Error Rate (QBER). The bits used for the estimation are discarded afterwards.

7) Finally, either Bob or Alice (in the case of direct or reverse reconciliation respectively) correct the errors with classical post-processing methods. After privacy amplification, both parties share a secure key that can subsequently be used to encrypt messages through the classical channel.

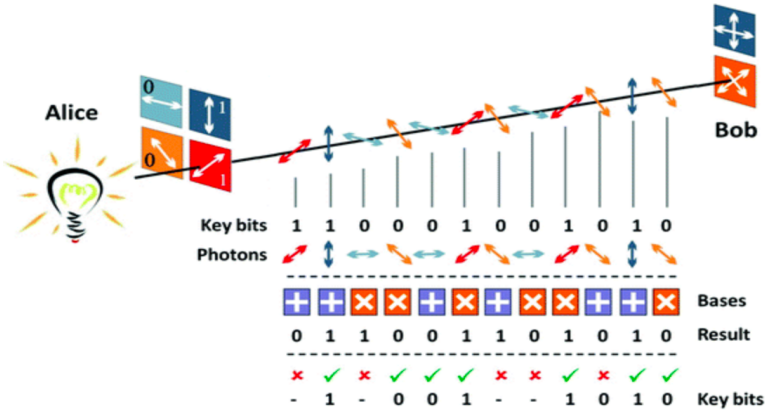


Figure 1.2: BB84 protocol, transmission and measurement scheme [21]

Alice and Bob will use the value of QBER estimated during step 6 to bound Eve's information. However, if they estimate an error rate that is too high, Eve has been present in the channel, and they will abort the protocol. Eve will be detected because as a consequence of the no-cloning theorem, she will not be able to duplicate the states Alice sends to Bob keeping one copy to herself. Instead, Eve will be forced to measure the state and then generate it again and send the fake new state to Bob. However,

since she does this before the sifting of the key, she too has to do as Bob and choose randomly the basis in which she will measure the states. 50% of the time she will be correct and will generate the right state for Bob but the other 50% she will be mistaken and when Alice and Bob compare their sifted keys, errors will appear where they chose the same basis, alerting them of the presence of the eavesdropper. The above is an example of a simple so-called intercept and resend attack.

Efficient BB84

Employing a regular BB84 protocol as described above has the issue that since both bases can be chosen with equal probability, half of the exchanged bits will be discarded after the sifting stage because Alice's and Bob's choices will not coincide. In order to improve this, a more efficient protocol can be employed. The choice of basis continues to be random but the probability of choosing each is substantially different [22]. One of the basis will be used for the exchange of the actual key and this will be chosen with very high probability q. The other basis will be selected less often and will be used to detect the presence of the eavesdropper.

Introducing this asymmetry significantly improves the efficiency of the protocol while maintaining its security. In order to do this, the error rate is estimated separately for each basis. The exchange is deemed secure only if both error rates are sufficiently low.

Two-decoy state BB84

Attenuated lasers are very commonly used to generate qubits for protocols such as this one because generating true single photons is hard. The problem however, is that in practice the equivalent quantum state instead of an actual single-photon state, is a coherent state with an average number of photons μ. This means however that there is a non-negligible probability of the order of μ^2 of an emitted pulse having multiple photons. This leaves the scheme vulnerable to what is called a photon number splitting (PNS) attack [23]. The way this attack is performed is that if Alice has sent a state in a multi-photon pulse, Eve can split the pulse and keep part of the photons while the rest of the pulse continues on its way to Bob. By performing delayed measurements on these photons, Eve obtains information about the state without having to destroy the part that goes to Bob and thus allowing her to remain undetected.

In order to counteract this type of attack a strategy has been proposed [24] employing decoy states. The technique consists on Alice sending pulses with different statistics, changing the mean number of photons per pulse randomly through the duration of the quantum exchange. Alice will share the statistics of each pulse with Bob during the sifting stage. Since Eve will interact with the pulses before that stage, she will have no knowledge of the pulses' statistics and Alice and Bob can estimate and monitor the parameters for each type of pulse. By determining the yield of the received state, as

well as the error for each type of pulse they can detect Eve is present whenever these values differ from the expected ranges.

The particular protocol we examine here is a two-decoy scheme with one of the decoys being a vacuum state. In this configuration, Alice will send three types of pulses: with probability p_μ she sends signal pulses with mean number of photons μ, with probability p_ν she sends a weak decoy with mean number of photons ν, and with probability $1 - p_\mu - p_\nu$ she sends a vacuum state as the other decoy.

With the specificities of the protocol having been introduced, we will now see how to estimate the secret key rate of an efficient two-decoy BB84 protocol.

Asymptotic key rate

As a first estimation of the secret key rate we compute an upper bound in the asymptotic regime, that is, assuming that we have an infinite stream of incoming qubits being received. The asymptotic key rate for this protocol [1] can be estimated as follows:

$$K_A = q\left\{Q_{\mu,0} + \mathbb{E}[Q_{\mu,1}][1 - h(\mathbb{E}[\epsilon_{\mu,1}]\mathbb{E}[Q_{\mu,1}])] - f_{EC}\mathbb{E}[Q_\mu]h(\epsilon_\mu)\right\} \tag{1.2.1}$$

The parameters involved in the equation are:
q denotes the probability of choosing the basis used for information exchange in an efficient protocol. In the asymptotic regime, it can be approximated to ~ 1. $\mathbb{E}[\cdot]$ corresponds to the expected value. f_{EC} denotes the efficiency of the error correcting code.

Q_μ, $Q_{\mu,1}$ and $Q_{\mu,0}$ are the gains of the signal state, the weak decoy and the vacuum decoy respectively. $Q_{\mu,1}$ is the gain of single photon states for the signal i.e. the joint probability of a detection in the event that Alice sent 1 photon in the pulse. $Q_{\mu,0}$ is the joint probability of a click when Alice sends 0 photons in the pulse. Q_μ is the total gain of the signal. They are defined as:

$$Q_\mu = 1 - e^{-\eta_d T^2 \mu}(1 - Y_0) \qquad Q_{\mu,1} = Y_1 \mu e^{-\mu} \qquad Q_{\mu,0} = Y_0 e^{-\mu} \tag{1.2.2}$$

These gains represent the number of detections for each type of state and depend on the detector efficiency η_d, the mean number of photons of the signal state μ, the transmission efficiency of the channel T and the yield Y_i. The latter is defined as the conditional probability of a detection given an $i-$photon state has been emitted and can be computed as $Y_i = 1 - (1 - Y_0)(1 - \eta_d T^2)^i$.

ϵ_μ corresponds to the total error rate of the signal and $\epsilon_{\mu,1}$ is the error rate of the pulses where Alice sends 1 photon:

$$\epsilon_\mu = \frac{1}{Q_\mu}(e_0 Y_0 + e_d(1 - e^{-\eta_d T^2 \mu})(1 - Y_0)) \tag{1.2.3}$$

$$\epsilon_{\mu,1} = \left[e_0 Y_0 + e_d(1-(1-\eta_d T^2))(1-Y_0)\right] \mu e^{-\mu}, \tag{1.2.4}$$

where $e_0 = 1/2$ is the probability of a background detection given that no pairs were emitted and e_d is the intrinsic error rate of the detector, which is usually defined as the probability that a photon hits the wrong detector.

Finally, we have the binary entropy function $h(x)$:

$$h(x) = -x\log_2(x) - (1-x)\log_2(1-x) \tag{1.2.5}$$

Computing the entropy for a given error rate gives us an estimation of the amount of information Eve has, allowing us to discard part of the key in order to ensure its secrecy.

Finite-size key rate

It is of interest to find an upper limit of the key rate through the asymptotic regime analysis, but a more precise estimation should take into account the effect of the finite sized nature of the qubit stream emitted by Alice. The key rate accounting for these effects [25] can be calculated as follows:

$$K_{FS} = \frac{1}{N}\left\{ s^L_{Z,0} + s^L_{Z,1}\left[1 - h(\phi^U_Z)\right] - \lambda_{EC} - 6\log_2\left(\frac{21}{\varepsilon_{sec}}\right) - \log_2\left(\frac{2}{\varepsilon_{corr}}\right)\right\} \tag{1.2.6}$$

N corresponds to the total number of bits sent during the exchange. λ_{EC} represents the amount of bits that were disclosed during the error correction procedures and must therefore be discarded. ε_{corr} is the correctness parameter, it indicates that the probability of Alice and Bob's keys being different is less than or equal to ε_{corr}. ε_{sec} is the secrecy parameter, it means that Eve has a probability lower than or equal to ε_{sec} of knowing the secret key. $s^L_{Z,1}$, $s^L_{Z,0}$ are the lower bounds on the number of pulses in which Alice sends respectively, 1 and 0 photons. Finally, ϕ^U_Z is an upper bound on the phase error rate of single photon events.

1.2.2 BBM92 protocol

The second protocol we will delve into was proposed by Bennett, Brassard and Mermin in 1992 [26]. This time, in addition to Alice and Bob a third party is also involved in the exchange, an untrusted source we will call Charlie, and we make use of another fundamental property of quantum mechanics, *entanglement*. The basic scheme of this protocol is illustrated in 1.3 and can be described as follows:

1) The third party Charlie, possesses a source capable of generating maximally entangled photon pairs (or EPR pairs) of the form : $|\Psi\rangle = \frac{1}{\sqrt{2}}(|H_A\rangle|V_B\rangle + |V_A\rangle|H_B\rangle)$ with $|H\rangle$ and $|V\rangle$ signifying photons with horizontal and vertical polarization respectively.

2) The two photons of each state are separated, one is sent to Alice and the other one is sent to Bob.

3) Similarly to step **3**) of the previous protocol, Alice and Bob independently and randomly choose a basis to measure each photon they receive. These measurement results constitute their *raw key*.

4) Alice and Bob then proceed to compare the bases they chose. They discard the elements of the key where their choices did not coincide. The remaining bits comprise the *sifted key*.

5) The remaining key bits should be perfectly correlated. In order to verify that, Alice and Bob share a portion of their key and estimate the error rate in the remaining key.

6) Finally, Alice and Bob perform error correction through their classical channel and discard any part of the key that may be known to Eve in a *privacy amplification* stage.

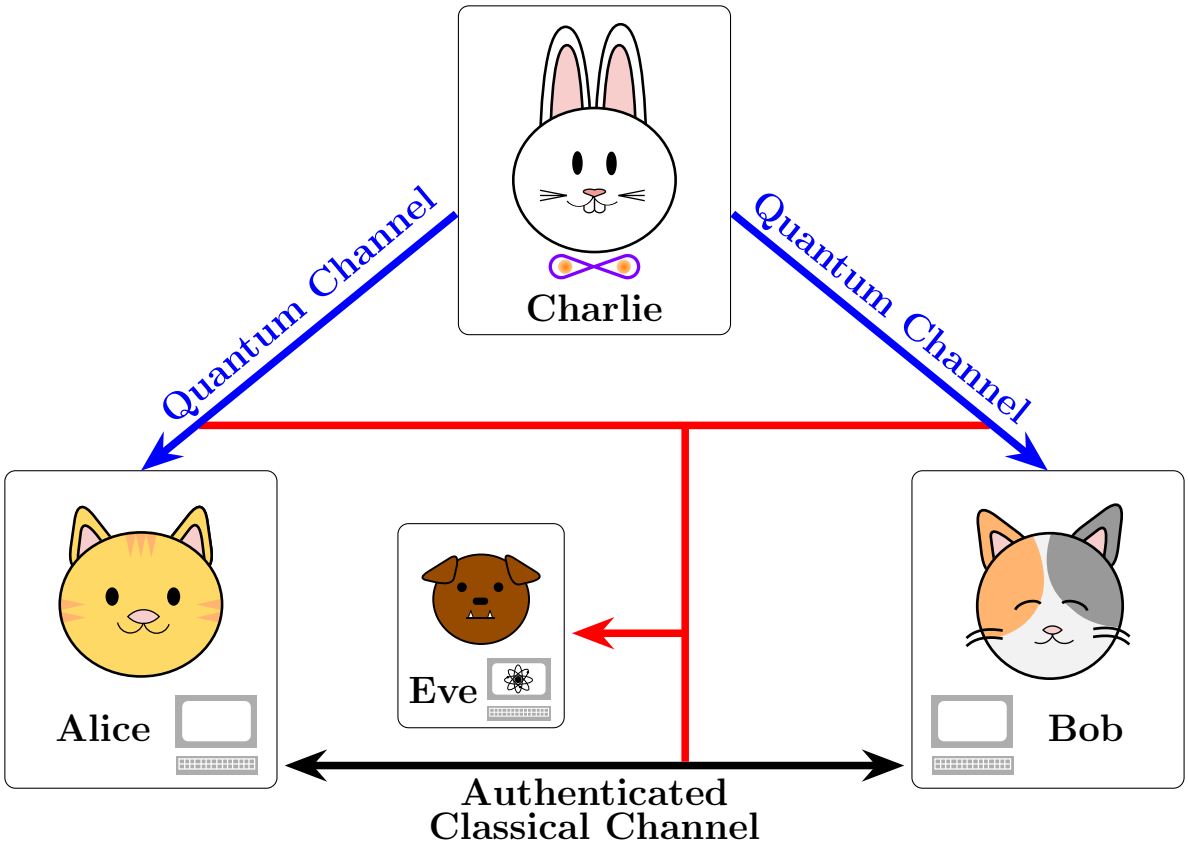


Figure 1.3: Entanglement-based QKD scheme

As is the case with the previous protocol, if Alice and Bob estimate an error rate that is too high in step **5)**, an eavesdropper is present, and the protocol will be aborted. Since it is much less likely to accidentally produce multiple entangled pairs correlated to one another than it is to generate a multiphoton pulse, the BBM92 protocol is significantly less susceptible to PNS attacks [1].

This protocol has two main advantages when compared to the previously discussed BB84: the first one is that a random number generator is not needed in order to produce the key bits, the randomness of the key is instead due to the probabilistic outcome of the measurement of the EPR state. The second one, is that Charlie can in theory be placed anywhere between Alice and Bob. If he were to be located inside Alice's lab for example, with her consuming one half of the pair and sending the other photon to Bob, it would be equivalent to a BB84 protocol. However, placing Charlie at an intermediary point could facilitate the establishment of keys through much longer distances since the distance each of the photons has to travel is only a portion of the total distance between Alice and Bob: roughly doubling the distance reached.

Asymptotic key rate

We estimate the key rate for this protocol in the asymptotic regime in order to obtain an upper bound. For this particular security bound, we assume that the entangled photon source to be used is of the parametric down conversion (PDC) [27] type. The key rate can be computed [28] through the following equation:

$$K_A = \frac{1}{2} R_c (1 - f_{EC} h(\epsilon) - h(\epsilon)) \tag{1.2.7}$$

Once again, h corresponds to the binary entropy function described in 1.2.5. f_{EC} corresponds to the efficiency of the error correction and ϵ is the error rate. The product of the latter two represents the amount of bits revealed by Alice and Bob for error correction which have thus to be discarded and R_c is the coincidence rate, that is, the rate at which both Alice and Bob will detect a photon, which can be described as:

$$R_c = \frac{1}{\Delta t} Q = \frac{1}{\Delta t} (p_0 Y_0 + (1 - p_0) Y_1) \tag{1.2.8}$$

Here, the gain $Q = p_0 Y_0 + (1 - p_0) Y_1$ defined as the probability of a coincidental detection for each pump pulse on the source; Δt is the temporal window in which a detection is possible. p_0 is the probability of no pairs having been emitted within that window.

We can consider that the PDC source emits entangled photon pairs with a probability that can be modelled as a Poissonian process [29] of mean μ. The probability of no pairs having been generated is therefore $p_0 = e^{-\mu \Delta t}$. Y_1 and Y_0 correspond to the so-called yields. The first one, is the conditional probability of a coincidental detection

event given that the source emitted a photon pair:

$$Y_1 = [1 - (1 - Y_{0A})(1 - \eta_A)] \cdot [1 - (1 - Y_{0B})(1 - \eta_B)] \tag{1.2.9}$$

Here, $\eta_{A(B)} = \eta_d T^2_{A(B)}$ is the efficiency of Alice(Bob) which includes the detector efficiency η_d and the transmission efficiency T^2.

The second yield, is the probability of a coincidental detection given that no photon pairs were emitted and corresponds to $Y_0 = Y_{0A}Y_{0B}$ with the individual 0-photon yields defined as:

$$Y_{0A(B)} = 1 - e^{-d_{A(B)}\Delta t}, \tag{1.2.10}$$

where $d_{A(B)}$ is the rate of dark counts.

The total quantum bit error rate ϵ necessary to estimate the key rate can be calculated as:

$$\epsilon = \left(\frac{1}{Q}\right)(e_0 Y_0 p_0 + e_1 Y_1 (1 - p_0)) \tag{1.2.11}$$

e_0 is the error rate corresponding to detections due to background noise, i.e. when no pairs were emitted. Due to its random nature, we can assume $e_0 = 1/2$. e_1 is the conditional probability of an erroneous detection given that a pair was indeed emitted, it can be estimated as:

$$e_1 = e_0 - \left(\frac{1}{Y_1}\right)(e_0 - e_d)\eta_A \eta_B, \tag{1.2.12}$$

where e_d is the probability that a received photon hits the wrong detector.

Finite-size key rate

The key rate estimated when taking into account the finite nature of the blocks of key being exchanged, can be computed through the following equation [30, 31].

$$K_{FS} = \frac{1}{T_b}\left[C_T - C_T h\left(\epsilon + \sqrt{\frac{(C_T + 1)\log_2(1/\varepsilon_{sec})}{4C_T^2}}\right) - C_T f_{EC} h(\epsilon) - \log_2\left(\frac{2}{\varepsilon_{corr}\varepsilon_{sec}^2}\right)\right] \tag{1.2.13}$$

T_b is the duration (in seconds) of each block of key that is sent. C_T corresponds to the total number of coincidental counts that are measured within that time for a given coincidence rate R_c. Similarly to the finite size analysis done for the previous protocol, ε_{corr} and ε_{sec} are the correctness and secrecy parameters of the final key.

1.3 Continuous variable QKD

The second main family of protocols that exist is the continuous variable quantum key distribution (CV-QKD). They differ from the DV-QKD protocols on a fundamental level since the information is no longer encoded into the discrete degrees of freedom of individual particles. Instead, the states shared between Alice and Bob can be coherent states coming from very attenuated laser pulses and modulated in amplitude and phase. The information of the key is in this case encoded into the quadratures of the electromagnetic field, similarly to many classical communication protocols.

The advantage of CV protocols in comparison with DV, comes down to technological implementation. High-efficiency single-photon receivers usually operate at ultra-low temperatures, necessitating bulky cooling systems. In contrast, CV employs laser sources and coherent detectors whose technology has been intensely developed throughout the last few decades for classical telecommunications applications, making them highly efficient at room temperature and already commercially available. However, the CV family of protocols also has its drawbacks, namely the fact that they are much more susceptible to losses. Since the information is encoded on the amplitude and phase of the pulse, and attenuation can alter these quadratures, the implementation of CV through large distances is severely limited.

In the following we will discuss in detail the steps and key rate estimation formulas of the GG02 or Gaussian modulation protocol.

1.3.1 Gaussian modulation protocol

The first version of a Gaussian modulation protocol was proposed in 2002 by Grosshans and Grangier [32]. It employs coherent quantum states with very few photons per pulse. Each state can be mathematically described as:

$$|\alpha\rangle = |q + ip\rangle \tag{1.3.1}$$

The general steps of the protocol are as follows:

1. For each state $|\alpha\rangle$ Alice wishes to send, she randomly and independently chooses the values of each one of the quadratures (q & p) from a Gaussian probability distribution as depicted in figure 1.4.

2. She generates a coherent state that she then be modulates in phase and amplitude. The phase and amplitude of the signal are determined by the quadrature values chosen in step 1. The phase corresponds to $arctan(p/q)$ and the amplitude is equal to $\sqrt{p^2 + q^2}$.

3. Alice sends the pulses and once Bob receives them, he measures them with a coherent detector. Bob either performs homodyne detection in which case he has

to randomly choose which of the quadratures he wishes to measure, or he uses a beam splitter and performs heterodyne detection to measure both quadratures.

4. Alice and Bob now share a set of correlated Gaussian variables from which they are able to extract the key, however they first need to go through a *parameter estimation* stage in which they calculate the amount of noise of the transmission as well as the transmissivity of the channel itself.

5. Having estimated the error rate of their exchange, Alice and Bob then go through an error correction stage called *reconciliation* process. Reconciliation can be *direct* if Bob corrects his information to match Alice's, or *reverse* if Alice is the one correcting her key in order to coincide with Bob's.

6. Finally, Alice and Bob will do some *privacy amplification* in which they will discard part of their shared information in order to ensure the secrecy of their key.

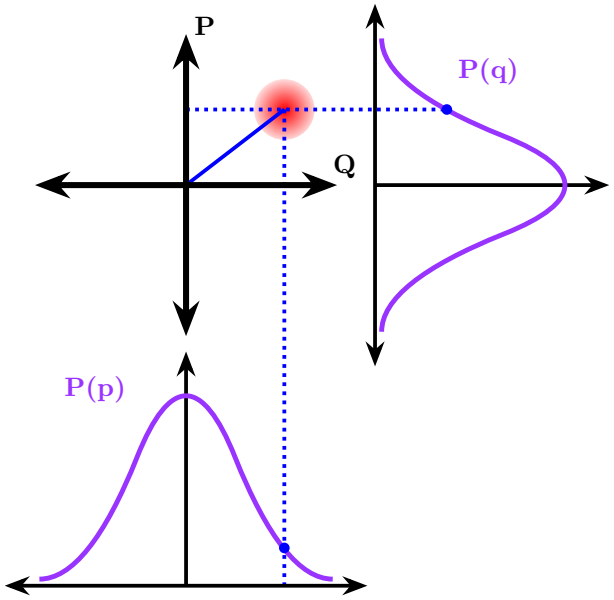


Figure 1.4: Gaussian modulation of coherent states

The coherent detection performed by Bob can be either homodyne or heterodyne. Homodyne detection only allows Bob to measure one of the quadratures p or q. This is done by mixing the received quantum state with a reference local oscillator (LO) in a 50:50 beam splitter and measuring the intensity at the output. The phase of the signal relative to the LO determines the quadrature in which the projective measurement is made. A phase shift of 0 on the signal, allows for the measurement of quadrature q while a phase shift of $\pi/2$ results in measurement of the quadrature p. Bob can then choose at random one of these phase shifts for each symbol he intends to measure which

would allow him to obtain partial information on the received states [33].

In contrast, heterodyne detection allows Bob to obtain information on both quadratures. To do that, the signal is divided in two by a 50:50 beam splitter, but instead of measuring the outputs directly, each one of them is sent into a homodyne detector. One homodyne detector will project the signal in order to measure quadrature q while the other applies a $\pi/2$ phase shift allowing for the measurement of p. With this measurement scheme, it is thus possible to obtain more information on the quantum state at the cost of the additional losses introduced by the initial splitting of the signal.

The parameters estimated in step 4 are an integral part of detecting the presence of an eavesdropper and gauging the amount of knowledge she may have on the key. As mentioned before in the text, the quadratures of a coherent state have a particular amount of uncertainty known as the shot noise; any noise detected beyond that and not modelled by the imperfections of the emission or transmission processes, will be attributed to Eve.

Going forward we will consider that Bob performs heterodyne detection and thus has access to both quadratures and that they are employing a reverse reconciliation scheme. Reverse reconciliation is favored in CV-QKD protocols because it has been demonstrated that using a direct reconciliation scheme when the channel loss is above 3 dB (as is our case) results in Eve potentially having more information on Alice's symbols than Bob does [33].

Asymptotic key rate

The way the key rate (in bits/symbol) is calculated in the asymptotic regime [34] for this protocol is as follows:

$$K_A = \beta I_{AB} - \chi_{BE} \tag{1.3.2}$$

The key rate is limited by the mutual information shared between Alice and Bob I_{AB} and the maximal amount of information Eve is estimated to have on the key, which is given by the Holevo quantity χ_{BE}. β is the efficiency of the reconciliation process between Alice and Bob.

The mutual information Alice and Bob share depends on the signal-to-noise ratio (SNR) and can be defined as:

$$I_{AB} = \log_2(1 + SNR) = \log_2\left(1 + \frac{\eta_d T^2 V_A}{2 + 2V_{el} + \xi T^2 \eta_d}\right) \tag{1.3.3}$$

T^2 is the transmission efficiency of the channel, η_d is the detector efficiency, V_A is the variance of the Gaussian distribution from which Alice has picked the quadrature values, V_{el} is the electronic noise of the detector and ξ is the excess noise related to

channel input that is attributed to Eve. $\sigma^2 = 2 + 2V_{el} + \xi T^2 \eta_d$ is the variance of the noise for a heterodyne measurement system.

The Holevo theorem [34] is a bound on the maximal amount of information Eve could have obtained for a given set of estimated parameters. It can be computed as:

$$\chi_{BE} = g(\nu_1) + g(\nu_2) - g(\nu_3) - g(\nu_4) \tag{1.3.4}$$

$\nu_{1,2}$ are the symplectic eigenvalues of the covariance matrix between Alice and the state just before the entrance of Bob's setup, and $\nu_{3,4}$ the symplectic eigenvalues of the covariance matrix of the state after Bob's measurement. They are determined by the variance V_A as well as the effects of the channel (η_d and T^2) [35]. In addition to that, the latter two eigenvalues are dependent on the noise measured by Bob after transmission. $g(z)$ is an estimation of the entropy defined as:

$$g(z) = \frac{z+1}{2} \log_2 \left(\frac{z+1}{2} \right) - \frac{z-1}{2} \log_2 \left(\frac{z-1}{2} \right) \tag{1.3.5}$$

Finite-size key rate

The computation of the finite-size key rate accounts for the effects of having only a limited amount of symbols exchanged from which to perform the parameter estimation. This is done through a pessimistic computation in which we consider the worst-case scenario for both the transmissivity and the noise of the channel [36]. The lower bound on the transmission of the channel and the upper bound on the noise variance can be found in the following equations:

$$T_{min} \simeq T - z_{\epsilon PE/2} \sqrt{\frac{1 + T^2 \xi}{m V_A}} \tag{1.3.6}$$

$$\sigma^2_{max} \simeq 1 + T^2 \xi + z_{\epsilon PE/2} \frac{(1 + T^2)\sqrt{2}}{\sqrt{m}} \tag{1.3.7}$$

m is the number of symbols used for parameter estimation and $z_{\epsilon PE/2}$ corresponds to:

$$z_{\epsilon PE/2} = \sqrt{2} \mathrm{erf}^{-1}(1 - \epsilon_{PE}) \tag{1.3.8}$$

where erf^{-1} is the inverse error function and ϵ_{PE} is the probability of failure of the parameter estimation.

1.4 Conclusion

In this chapter we have seen the motivation for QKD as well as the physical principles and description of three different protocols belonging to the main families of QKD, discrete and continuous variable. We also presented the methods of calculating the main performance metric we will take into account further on in our analysis, the secret key rate. So far we have assumed a quantum channel of fixed attenuation as is the case for optical fiber. In the following, we will examine how a channel with fluctuating losses as is the case for atmospheric propagation, can be modelled.

Chapter 2

Atmospheric channel propagation and adaptive optics correction

An optical wave propagating through the atmosphere will encounter in its path turbulent regions. There, it encounters temperature variations that induce a variation in refractive index which will result in phase perturbations in the propagated wave. Therefore, what could otherwise be modelled as a plane wave at reception is instead a distorted wavefront. In this section we will first detail the effects of atmospheric propagation and how the turbulent channel is modelled. Then we will see how a perturbed wavefront affects signal coupling into a single mode fiber and how other atmospheric effects like absorption and scattering can impact light collection in an aperture.

2.1 Propagation through atmospheric turbulence

The main processes that affect an optical wave when propagating through the atmosphere are: absorption and scattering that will result in an attenuated signal at reception, and temperature induced refractive index fluctuations [37]. The latter is the one we will focus on first.

The atmosphere is filled with physical phenomena of varying degrees of predictability, turbulence for example is a highly chaotic random process. It consists of air motion caused by convection and wind causing random temperature variations that end up resulting in fluctuations of the refraction index. In order to describe this process, Kolmogorov proposed the idea of a so-called energy cascade [38]. It proposes the idea of turbulence structures (or eddies) of decreasing size where the bigger ones gradually transfer their energy to the smaller structures. This goes on until due to air viscosity, the energy from the smallest structures closer to the ground ends up being transformed into heat.

If we consider turbulence to be stationary at a given time in very small regions, it is possible to describe it through statistics. Spatially, turbulent eddies will be limited by

what is called the outer and inner scales, corresponding to the size of the biggest and smallest turbulence whirlpools respectively. The values both of these scales take will vary depending on the altitude at which the atmosphere is being considered. The outer scale can go from a few meters to several tens of meters, we will consider it constant and equal to 5 m.

The values of most parameters related to atmospheric turbulence will depend significantly on the specific location on earth. Latitude, vegetation, time of day, wind and other climatic conditions will all influence the behavior of a wave propagating. The refractive index structure constant C_n^2 characterizes the turbulence strength locally, and it varies with altitude. The troposphere is the lowest layer of the atmosphere and is separated from the layers above by the tropopause. The exact altitude at which the tropopause is found depends on geographical location, but it is approximately 20 km, C_n^2 values above this altitude can be considered to be negligible.

Different models for this function have been proposed, such as the Hufnagel-Valley heuristic model [39]. This one depends on the distance from the ground h, the value of the structure constant measured at ground level C_0, and the wind speed $V_(z)$ which will affect the turbulence strength at high altitude. Nevertheless, this model is limited, hence why we decided to construct our own C_n^2 turbulence profiles which we will explain in section 2.1.1

As was the case with the C_n^2, multiple models also exist to describe the evolution of the wind speed, in the case of optical wave propagation where both source and observer are static or move at negligible speeds the apparent wind is determined by the natural wind speed. We will consider the Bufton model [40]:

$$V_{nat}(h) = V_G + V_T e^{((h_T - h)/D_T)^2} \tag{2.1.1}$$

V_G is the wind speed at ground altitude, V_T is the speed of the wind at the tropopause, and h_T and D_T correspond to the altitude, and the thickness of the tropopause respectively which depend on the geographic location. For the estimation of the natural wind, in our study we take the wind speed at ground level to be $V_G = 10$ m/s and the wind speed at the Tropopause $V_T = 25$ m/s.

However, in the case of a LEO satellite the wind $V(z)$ includes not only the previously explained natural wind, but also the apparent wind induced by the satellite moving across the sky. This apparent wind, which is the dominant effect, is defined as $V_{app}(z) = \dot{\theta} z$ with z being the distance to the satellite and $\dot{\theta}$ the slew rate of the satellite being $\dot{\theta} = V_{orth}(\varepsilon)/R(\varepsilon)$. Here, $R(\varepsilon)$ is the distance to the satellite at elevation ε and V_{orth} is the component of the satellite speed (V_{sat}) which is orthogonal to the line of sight, and for a circular orbit passing at the zenith it depends on the elevation, Earth's

radius R_E and the satellite altitude h_s as such:

$$V_{orth}(\varepsilon) = V_{sat}\sqrt{1 - \left(\frac{R_E\cos(\varepsilon)}{R_E + h_s}\right)^2} \tag{2.1.2}$$

While the C_n^2 estimates the evolution of the refractive index along the optical path, there is a series of parameters derived from it that give a better perspective of the effects on the optical signal after propagation through the entire line of sight. These are the so-called integrated parameters, the Fried parameter, the coherence time, and the isoplanatic angle.

The Fried parameter r_0 characterizes the strength of the turbulence along the line of sight [41]. It can be interpreted as a measure of the energy of the turbulence or as the area in which the optical field is coherent under the atmospheric conditions considered. It can be calculated as [42]:

$$r_0 = \left[0.423\left(\frac{2\pi}{\lambda}\right)^2 \int_0^{z_{max}} C_n^2(h(z))dz\right]^{-3/5} \tag{2.1.3}$$

Here, z is the distance to the turbulent volume, $h = z\sin(\varepsilon)$ determines the altitude of the atmospheric layer with ε the elevation angle from the horizon. λ is the wavelength of the optical wave and z_{max} the distance corresponding to the tropopause boundary where C_n^2 becomes negligible.

The correlation time τ_0 is a temporal characterization of the turbulent wavefront. It can be computed through the following equation:

$$\tau_0 = \left[2.91\left(\frac{2\pi}{\lambda}\right)^2 \int_0^{z_{max}} V(z)^{5/3} C_n^2(h(z))dz\right]^{-3/5} \tag{2.1.4}$$

The temporal representation of the turbulent path can be modelled either through the correlation time τ_0 or the Greenwood frequency f_G, with the relation between the two being $\tau_0 = 0.134/f_G$ [43].

The isoplanatic angle θ_0 characterizes the angular decorrelation of the wavefront [43], it is defined as the angle at which the mean-square error between two wavefronts $E([\phi(r,0) - \phi(r,\theta_0)]^2)$ is 1 rad^2. It can be interpreted as the angular separation at which two wavefronts can be considered to be significantly different. We can calculate it through the following equation:

$$\theta_0 = \left[2.91\left(\frac{2\pi}{\lambda}\right)^2 \int_0^{z_{max}} z^{5/3} C_n^2(h(z))dz\right]^{-3/5} \tag{2.1.5}$$

In the case of a LEO satellite, the interest of knowing the isoplanatic angle lies in the fact that it can be used to estimate the coherence time as $\tau_0 \approx \theta_0/\dot{\theta}$.

2.1.1 Turbulence profile generation

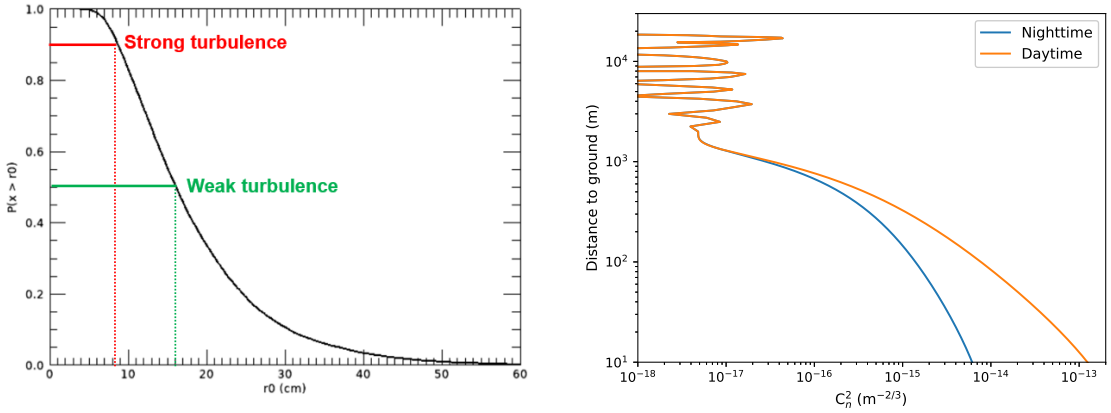
A turbulence profile corresponds to the evolution of the C_n^2 structure constant with respect to altitude. Through the following method [44], we generate statistically representative turbulence profiles to be used as reference cases for our studies. It gives an idea of the turbulence conditions under which the scenarios and protocols we consider could be feasible.

In order to do so, a series of approximations are to be made. First, the integrated parameters θ_0 and r_0 are considered to be mostly independent. The former is determined mainly by the atmosphere at high altitudes (above 2000 m), while the latter depends mostly on the lower layers of the atmosphere. These two parameters and the accompanying assumptions are the base upon which our profiles are constructed.

We employ experimental measurements from different astronomical sites in order to build the set of C_n^2 we work with. The turbulence profiles obtained at the end will be hybrids, combining the measurements from two databases, with different ones being used for day or night profiles.

We start with the upper layers of the atmosphere. We have access to a large amount of C_n^2 measurements taken at Cerro Paranal [45] and we estimate the value of θ_0 for each profile. Then, we compute the probability distribution of the parameter. Next, we decide on a threshold for the value of θ_0 according to the turbulence we wish to represent. For example, we can decide to use a θ_0 value corresponding to the lower quartile of the probability distribution meaning that in 75% of the cases, the isoplanatic angle would be higher than the value we have chosen. The high altitude Cn^2 profile we will proceed with is the one with the θ_0 value closest to that corresponding to the chosen threshold.

The low atmosphere C_n^2 values are derived from two different Canary Islands databases, for daytime we had C_n^2 measurements at 30 m altitude already available [46]. In order to analyze nighttime turbulence conditions as well, we selected a new database containing seeing values at night [47]. The behavior of C_n^2 for the low layers is deduced using a Monin-Obhukov similitude law which describes the evolution of this parameter on the surface layer as a function of height. When combined with the previously chosen high altitude layers, this results in a large set of hybrid profiles. As was done before, a probability distribution is derived, only this time it corresponds to the distribution of the r_0 values of the hybrid profiles. A threshold is chosen as depicted in figure 2.1a and the resulting turbulence profile will correspond to the hybrid profile with the Fried parameter associated to the selected threshold.



(a) r_0 inverse probability distribution (b) Resulting turbulence profiles

Figure 2.1: Result examples of the turbulence profile construction process.

Examples of the resulting daytime and nighttime turbulence profiles at the zenith can be found in figure 2.1b and will have around 1000 C_n^2 values for different atmospheric layers. As a final step, we deduce the profile along the line of sight at a given elevation, and we perform a downsampling in order to ease computations when used in simulation.

2.2 Wavefront aberrations

The impact of turbulence on a wave propagated through the atmosphere can be expressed as:

$$\Psi = \Psi_0 e^{\chi + i\varphi} \tag{2.2.1}$$

Where Ψ_0 corresponds to the undisturbed wave and χ and φ will model the amplitude and phase perturbations respectively.

χ is the so-called log-amplitude parameter, it is a measure of scintillation, that is, the local fluctuation of amplitude caused by turbulence. Assuming we are in the weak perturbation regime, the variance of the log-amplitude parameter at a given point of the receiver pupil can be calculated as [48]:

$$\sigma_\chi^2 = 0.5631 \left(\frac{2\pi}{\lambda}\right)^{7/6} \int_0^{z_{max}} z^{5/6} C_n^2(h) dz \tag{2.2.2}$$

χ will vary spatially through the receiving aperture and if the aperture is large enough the effects of scintillation can end up being averaged out. If we consider a given

diameter $D >> \sqrt{\lambda z}$ [49], the scintillation variance over a given aperture is:

$$\sigma_{\chi D}^2 = \frac{4.34}{D^{7/3}} \int_0^{z_{max}} z^2 C_n^2(h) dz \tag{2.2.3}$$

The weak perturbation regime, in which we will consider to be going forward, corresponds to a fluctuation of the intensity of the wave with variance $\sigma_\chi^2 < 0.3$ [50].

φ represents the phase aberrations of the optical wave, its variance over an aperture of diameter D in the absence of correction is:

$$\sigma_\varphi^2 = 1.03 \left(\frac{D}{r_0}\right)^{5/3} \tag{2.2.4}$$

2.2.1 Zernike polynomials

It is important to note that φ corresponds to the phase in the pupil at a given time t. It refers to the evolution of the wavefront in space and can be modelled in different ways, one of the most common ones being the decomposition in Zernike polynomials. This is particularly useful when trying to reconstruct the wavefront at reception or when trying to correct some of the turbulence's effects. The polynomials constitute an orthogonal basis in the unit radius disk and the expansion of the phase in the Zernike modes can be described as follows:

$$\varphi(r, \theta) = \sum_{j=1}^{\infty} \varphi_j Z_j(r, \theta) \tag{2.2.5}$$

The Zernike coefficient φ_j, is a projection of the wavefront on the j-th Zernike polynomial. Z_j are the Zernike polynomials and can be calculated as follows [48].

$$\begin{aligned} \text{For j even}: \quad & Z_j = \sqrt{n+1} R_n^m(r) \sqrt{2} \cos(m\theta), \quad m \neq 0 \\ \text{For j odd}: \quad & Z_j = \sqrt{n+1} R_n^m(r) \sqrt{2} \sin(m\theta), \quad m \neq 0 \\ & Z_j = \sqrt{n+1} R_n^0(r), \qquad m = 0 \end{aligned} \tag{2.2.6}$$

m corresponds to the azimuthal frequency and n denotes the radial order. $R_n^m(r)$ are the radial polynomials and can be defined as:

$$R_n^m(r) = \sum_{k=0}^{(n-m)/2} \frac{(-1)^k (n-k)!}{k! \left(\frac{(n+m)}{2} - k\right)! \left(\frac{(n-m)}{2} - k\right)!} \quad r^{n-2k} \tag{2.2.7}$$

Figure 2.2 shows the visualization of the ten first Zernike polynomials with their respective radial orders. Each polynomial or mode corresponds to an optical aberration. Mode Z_1 for example, is the piston mode and corresponds to a constant global phase

shift. Modes $Z_{2,3}$ are the *tip* and *tilt*, most ground stations used for satellite-to-ground communications are equipped with compensation for these two modes.

The correction capabilities of an adaptive optics system can be characterized by the number of radial orders n_r it is able to correct. A system able to correct n orders will compensate up to the mode Z_{j-max} with $j_{max}(n) = j_{n+1} - 1 = \frac{(n+1)(n+2)}{2}$, where j_{n+1} is the Zernike number of the first mode of radial order $n + 1$.

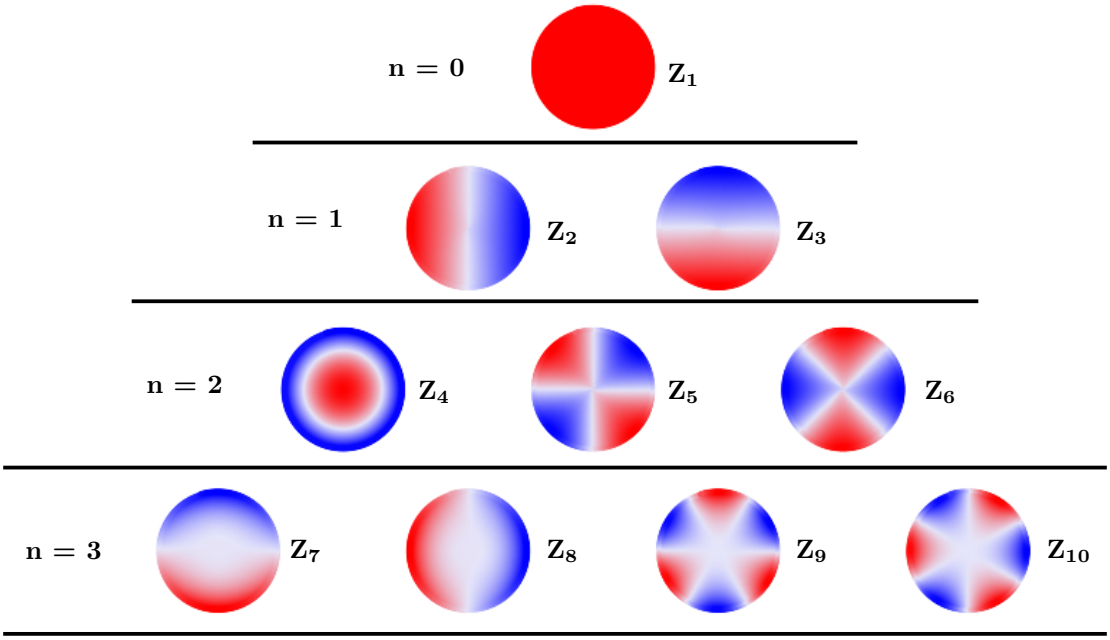


Figure 2.2: First 10 Zernike polynomials Z_j.

In order to find the value of the Zernike coefficients φ_j, the turbulent wavefront can be projected into each of the Zernike polynomials. Through said coefficients, the variance of the phase of the turbulent wave from equation 2.2.5 can be described as follows:

$$\sigma_\varphi^2 = \sum_{j=2}^{\infty} \varphi_j^2 \tag{2.2.8}$$

Since the global phase of the unperturbed emitted wave is not usually known to the receiver, it is not possible (at least by employing an adaptive optics system) to measure and thus correct the piston mode Z_1, hence why it is not included in the estimation of the variance of the turbulent wavefront.

2.2.2 Single mode fiber coupling

Coupling a signal that has been propagated through the atmosphere into a single mode optical fiber (SMF) can sometimes be very useful. In the domain of free-space classical communications as well as continuous variable quantum communications, single mode coherent receivers are commonly used. The principle of coherent reception is to mix the received signal with a local oscillator in order to perform detection. This process is significantly easier to execute when both signal and oscillator are inside optical fibers. On the other hand, while discrete variable QKD can be performed entirely in free-space, fiber coupling allows access to highly efficient state-of-the-art superconducting nanowire single photon detectors (SNSPD).

However, it is not possible to fit all the received signal into an SMF, in particular after it has been affected by atmospheric propagation. In order to estimate the portion of the received light that can be coupled we can calculate the overlap integral between the two waves [51]:

$$CE = \left| \frac{\int A_1(\mathbf{r}) A_2^*(\mathbf{r}) d\mathbf{r}}{\sqrt{\int |A_1(\mathbf{r})|^2 d\mathbf{r}} \sqrt{\int |A_2(\mathbf{r})|^2 d\mathbf{r}}} \right|^2 \tag{2.2.9}$$

CE denotes the coupling efficiency, it corresponds to the square norm of the coupling between two complex signals $A_1(\mathbf{r})$ and $A_2(\mathbf{r})$ where $\mathbf{r}$ is the two-dimensional coordinate vector. We take $A_1(\mathbf{r})$ to be the incoming wave after atmospheric propagation as described in equation 2.2.1 and cropped by the receiving telescope circular aperture of diameter D. $A_2(\mathbf{r})$ is the optical mode corresponding to the SMF. It is important to note that this coupling efficiency is normalized with respect to the so-called power in the bucket, i.e. the optical power in the receiving aperture.

In order to maximize the coupling into the SMF, the focal point of the receiving aperture is adapted in such a way that $D/w(z_{CE}) = 2.2$. Here $w(z_{CE})$ is the waist of the fiber mode at the pupil, which will be located at distance z_{CE} from the fiber [52]. Without atmospheric aberrations and assuming a completely flat wavefront, the maximal coupling efficiency of a flat wavefront with an optical fiber is 81%.

2.2.3 Adaptive optics

Nevertheless, that maximal coupling efficiency will not be reached in practice since there will always be some degree of aberration in the optical signal. In order to mitigate this detriment to the performance, real time correction by adaptive optics can be implemented. An example of a generic adaptive optics (AO) system can be observed in figure 2.3.

This type of systems work by implementing a feedback loop. The incoming signal is reflected by a deformable mirror (DM) and then passes through a beam splitter that is redirected to a wavefront sensor (WFS). The sensor will measure the difference between the residual wavefront after correction and a reference wavefront (generally a flat wavefront) and a real-time computer (RTC) will send commands to the DM in order to minimize the deviation from the reference wavefront. The rest of the optical power after the beam splitter is then coupled into a single-mode fiber.

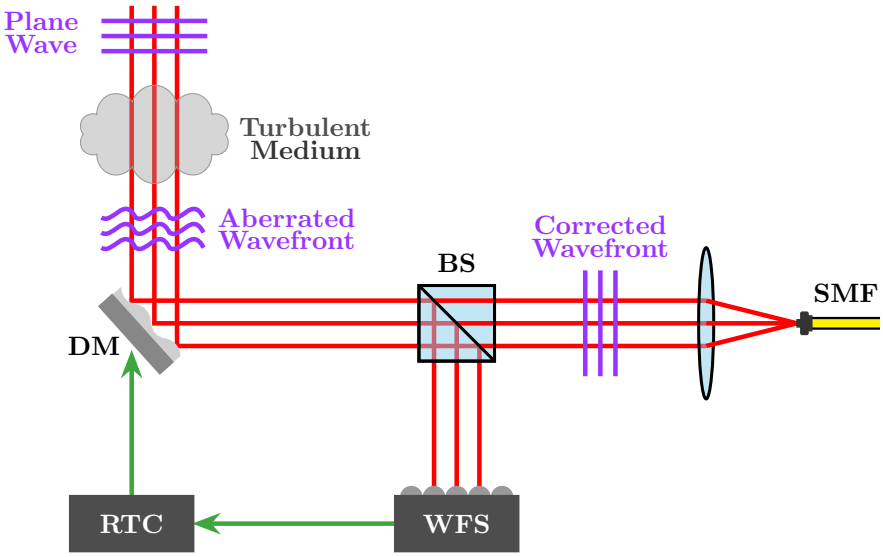


Figure 2.3: General scheme of an adaptive optics system. WFS: Wavefront sensor, DM: Deformable mirror, RTC: Real time computer, BS: Beam splitter.

In the following we will explain the basic operating principle of the main components of an adaptive optics system, later on we will associate each of them to a source of error responsible for the total residual phase after correction.

Wavefront sensor

In order to be able to correct the perturbed wavefront it is first necessary to be able to measure its aberrations. One of the most commonly used wavefront sensors is the so-called Shack-Hartmann wavefront sensor, its basic functioning principle is as follows. It is composed of an array of lenses which results in an array of images in a detector. The matrix of lenses, or sub-apertures, is used to sample the wavefront spatially. Each lens will focus a portion of the received wave into a corresponding section of pixels in the detector. For a plane wave each section of light will focus exactly at the center of the pixel zone and any deviation from the center allows for the measurement of the local phase slope. The measurement of all the slopes from the detector matrix allows for a reconstruction of the received wavefront [53]. Said reconstruction is not perfect: the final spatial sampling given by the sub-apertures limits the number of Zernike modes

that can be reconstructed and induces an aliasing effect, leading to the so-called aliasing error.

Deformable mirror

Once the wavefront aberrations have been properly measured, it is necessary to actively correct them. For that, instead of reflecting the optical signal with a regular mirror to redirect it to the sensor, a deformable mirror is used. This usually consists of a continuous reflective membrane under which several actuators are placed. The actuators can be piezoelectric or magnetic devices that can be addressed individually in order to perform a force displacing the membrane. The instructions to the DM are designed in such a way that it compensates the remaining measured aberrations, obtaining a less perturbed wavefront after reflection [53]. The displacement commands are therefore incremental and relative to the current position of the actuators.

The device is imperfect, resulting in a fitting error, that depends mainly on the number of actuators present. In order to avoid limiting ourselves to a specific mirror architecture, we will consider a simplified model with an ideal device characterized by the number of Zernike modes it is able to correct.

Real-time computer

A computer is necessary within the system in order to connect the other two main components. Its main purpose is to translate the wavefront sensor's slope measurements into commands for the deformable mirror actuators. It holds as well the algorithms in order to control the feedback loop. We consider here an integral controller characterized by its gain g. The transfer function of the feedback loop will ultimately be determined by the actuators influence on the mirror surface, the gain of the controller and the wavefront measurements.

Since turbulence varies in time, the system will have to actively compensate for aberrations in real time, that is, the system has to be able to correct faster than the characteristic time of the turbulence. The feedback loop being imperfect, there is a residual error mainly induced by the temporal delay inherent to the loop. In addition, it takes a non-negligible amount of time to read the WFS data and do the calculations necessary to transform measurements into commands. Overall, there is a delay between the wavefront being measured and the one being corrected leading to a temporal error.

2.2.4 Simplified Adaptive Optics Simulation (SAOST)

The simplified adaptive optics simulator is a pseudo-analytic performance evaluation tool developed at ONERA that allows us to estimate the effect of a given turbulence profile on the coupling efficiency and its partial correction through AO [54, 55]. SAOST

assumes a plane wave arrives at the turbulent volume and thus in the absence of turbulence a plane wave arrives at the receiving pupil. It is used to estimate the proportion of received light actually coupled into the fiber (disregarding geometrical losses) in the context of optical communication between ground stations and satellites. It can produce either a probability distribution or a time series of coupling efficiency values for a given set of parameters [55]. Said parameters include a turbulence profile, the distance and elevation angle of the satellite and the correction capabilities of the adaptive optics system. The AO feedback loop considered assumes an integral control algorithm with gain $g = 0.5$ and two frames of delay.

The wavefront occurrences are produced by modelling the residual phase after AO correction through an error budget estimation. It works by performing a Monte-Carlo style simulation where numerous random occurrences of received flux are produced. For each occurrence, the coupling efficiency is computed as per equation 2.2.9, if a sufficiently large number of occurrences are generated, a statistical representation of the channel can be derived.

Error budget

The variance of the phase of a wave affected by turbulence is given by equation 2.2.4. The use of an adaptive optics system will however, only partially correct *some* of these aberrations. In order to estimate the efficiency of the coupling into the fiber it is important to model the errors of the system and thus what the residual phase error is after correction. This being intended to be a fast tool, these error terms are based on simplified models in order to facilitate the calculations. The residual phase variance is described as follows:

$$\sigma^2_{res} = \sigma^2_{fit} + \sigma^2_{alias} + \sigma^2_{tempo} \tag{2.2.10}$$

We can see that this error budget includes one type of error from each of the three main components of an AO system. The first one is the fitting error, it is caused by the finite number of actuators of the deformable mirror. In our case we consider that only a finite number of Zernike modes can be corrected by the system, the fitting term is therefore the variance of the uncorrected high order terms.

In order to not limit the analysis to a specific deformable mirror technology or arrangement, we model the limitations of the system by the number of Zernike radial orders it is capable to correct n_r. The fitting error will be determined by the turbulence conditions through the Fried parameter r_0, and the diameter of the receiving aperture D. The fitting error is given by:

$$\sigma^2_{fit} = 0.458(n_r + 1)^{-5/3} \left(\frac{D}{r_0}\right)^{5/3} \tag{2.2.11}$$

The second source of error considered is the aliasing error. The wavefront sensor has a finite number of sub-apertures, hence a finite spatial sampling leading to aliasing effects. The aliasing error with a modal distribution found in [56], can be approximated as the following:

$$\sigma^2_{alias} \approx 0.35 \cdot \sigma^2_{fit} \tag{2.2.12}$$

The last error contribution taken into account corresponds to the temporal error that is related to the characteristics and inherent delay of the feedback loop. This error represents the fact that due to the time it takes to process measurements and commands, the wavefront being acted upon is slightly different from the one that was measured. The temporal error can be estimated as the sum of the temporal errors of all corrected radial orders n_r:

$$\sigma^2_{tempo} = \sum_{n=1}^{n_r} \sigma^2_n \tag{2.2.13}$$

The residual phase error variance of each radial order composed of the Zernike modes j_n to $j_{n+1} - 1$ can be calculated as:

$$\sigma^2_n = \sum_{j=j_n}^{j_{n+1}-1} \int_0^\infty RTF(f) PSD_j(f) df \tag{2.2.14}$$

PSD_j corresponds to the power spectral density of Zernike mode j, f is the temporal frequency and RTF is the rejection transfer function, it is a measure of the correction provided by the feedback loop and can be expressed as:

$$RTF(f) = \left| \frac{1}{1 + L(f)} \right|^2 \tag{2.2.15}$$

Where $L(f)$ corresponds to the open loop transfer function which will be the product of the transfer functions of each main component of the system. This will account for the integral control algorithm and the two frames of delay of the real-time system.

Some other sources of error exist but are not taken into account here for the sake of simplicity. The measurement noise of the wavefront sensor for example, can be neglected if we assume that the signal used for the measurement has a strong enough flux [57].

This simulation tool while simplified, is able to efficiently and accurately estimate the effect of the channel and AO correction on the optical signal. The results obtained through SAOST have been proven to be consistent with more detailed and computationally complex simulators modelling the end to end transmission through phase screens [54, 55, 58].

2.3 Atmospheric effects beyond turbulence

Turbulence is not the only atmospheric effect that will impact the optical signal during propagation. Diffraction, absorption and scattering will play a key role in the losses of the atmospheric channel. In addition to that, it is possible for the light beam to not be perfectly pointed towards the receiver, resulting in less light captured inside the aperture and thus even higher losses.

2.3.1 Geometric losses and beam wandering

Geometric losses, also known as path loss, are the main contributing factor (in terms of magnitude) to the attenuation of the optical signal. They depend on the propagation distance and are linked to the divergence of the beam. We model the source as a Gaussian beam non-truncated by the emitter aperture.

The electromagnetic field of a Gaussian beam propagating in the direction z, can be defined as:

$$E(r,z) = \frac{w_0}{w(z)} \exp\left(\frac{-r^2}{w(z)}\right) \exp\left(-i\left[kz + k\frac{r^2}{2R(z)}\right]\right) \tag{2.3.1}$$

$k = 2\pi/\lambda$ is the wave number, λ the wavelength, w_0 is the beam waist, it corresponds to the radius of the beam at the origin (z=0). The waist of the Gaussian beam at different points in the propagation path can be calculated as follows:

$$w(z) = w_0\sqrt{1 + \left(\frac{z\lambda}{\pi w_0^2}\right)} \tag{2.3.2}$$

It is important to note that in addition to the beam emitted by the satellite source, we can also model the mode of a single-mode optical fiber as a Gaussian beam, in this case the waist parameter can be defined as $w_0^{SMF} = 2\text{MFD}$, with the mode field diameter (MFD) of a single mode fiber for a 1550 nm wavelength being around 10μm.

The curvature radius of a Gaussian beam can be estimated for all points of the trajectory as:

$$R(z) = z\left[1 + \left(\frac{\pi w_0^2}{z\lambda}\right)\right] \tag{2.3.3}$$

The transmission efficiency of the atmospheric channel taking into account only the geometric loss of a Gaussian beam can be calculated as [59]:

$$T_0^2 = 1 - \exp\left(-2\frac{D^2}{4W_z^2}\right) \tag{2.3.4}$$

D once again corresponds to the diameter of the receiver aperture and W_z is the waist of the Gaussian beam in the reception pupil plane, at the ground in our case, it

can be approximated as $W_z = \theta_d R$ with R the total distance of the propagation trajectory and θ_d the divergence of the beam. Said divergence can be defined as $\theta_d = \frac{\lambda}{\pi w_0}$ where it is a function of the w_0 waist of the beam at its origin, in our case aboard the satellite.

The above is valid if the light beam and the receiver telescope are perfectly aligned which is not always the case. The light beam may wander from its intended reception point and this will affect the collection of light leading to more losses. This beam wandering has two main causes, turbulence effects may displace the beam randomly and the pointing system of the emitter may have some jitter error. The probability distribution of the center of the optical beam being at distance r from the center of the aperture can be found in equation 2.3.5.

$$P(r) = \frac{r}{\sigma_r^2} \exp\left(-\left(\frac{r}{\sqrt{2}\sigma_r}\right)^2\right) \tag{2.3.5}$$

This is a Weibull probability distribution with zero mean and a standard deviation σ_r determined by:

$$\sigma_r = \sqrt{(R\theta_p)^2 + \sigma_{turb}^2} \approx R\theta_p \tag{2.3.6}$$

σ_{turb}^2 is the variance of the deflection distance that's caused by turbulence effects. In the case of an optical transmitter on board of a satellite however, pointing error is quite significant (of the order of μrad) and thus the value of σ_{turb}^2 becomes negligible when compared to the variance due to the pointing jitter. The latter of which will be proportional to the propagation distance R, over hundreds of kilometers for LEO satellite-to-ground transmission, and the standard deviation of the pointing error θ_p resulting in σ_r being on the order of several meters.

Having modelled the probability distribution of the deflection distance r, the transmission efficiency of the atmospheric link taking into account path loss and beam wandering can be estimated as [59]:

$$T^2 = T_0^2 \exp\left(-\left(\frac{r}{\beta}\right)^\alpha\right) \tag{2.3.7}$$

α and β are the shape and scale parameters whose expressions can be found in equations 2.3.8 and 2.3.9 respectively. I_i corresponds to the i-th modified Bessel function.

$$\alpha = 2\frac{D^2}{W_z^2} \cdot \frac{\exp\left(-\frac{D^2}{W_z^2}\right) I_1\left(\frac{D^2}{W_z^2}\right)}{1 - \exp\left(-\frac{D^2}{W_z^2}\right) I_0\left(\frac{D^2}{W_z^2}\right)} \cdot \left[\ln\left(\frac{2T_0^2}{1 - \exp\left(-4\frac{D^2}{4W_z^2}\right) I_0\left(\frac{D^2}{W^2}\right)}\right)\right]^{-1} \tag{2.3.8}$$

$$\beta = \frac{D}{2}\left[\ln\left(\frac{2T_0^2}{1-\exp\left(-4\frac{D^2}{4W_z^2}\right)I_0\left(\frac{D^2}{W^2}\right)}\right)\right]^{-1/\lambda} \tag{2.3.9}$$

2.3.2 Absorption and scattering

Absorption and scattering effects will also contribute to the attenuation of the signal, however, they are very dependent on sky conditions. Multiple computational models exist, including MODTRAN [60], the Moderate resolution atmospheric transmission computer code. It consists of a series of complex algorithms that calculate how light interacts with different sized particles present in the atmosphere. It takes into account the wavelength of the optical signal, different visibility conditions as well as different atmospheric models depending on things like latitude and weather.

With MODTRAN, it is possible to obtain the zenith transmission efficiency τ_{zen} due to absorption and scattering effects for certain climatological conditions. In order to adapt this zenithal value to other elevation angles ε, we can compute this contribution to the transmission efficiency as:

$$\tau_{atm} = \tau_{zen}^{sec(\frac{\pi}{2}-\varepsilon)} \tag{2.3.10}$$

2.4 Conclusion

The simulation tools and analytical expressions employed to represent the behavior of the channel are constructed from detailed models either based on experimental data, as is the case for the turbulence profiles, or validated through real measurements as happens with SAOST. For the latter, in addition to in-lab demonstrations, measurements taken during an experimental campaign [54], are shown to be coherent with SAOST simulation results. While the geometry considered is different from the one taken into account in this manuscript, the statistics related to turbulence effects are consistent with simulation showing that this tool gives results representative of real turbulence conditions.

The combination of the turbulence and adaptive optics simulation via SAOST and the path loss and absorption effects described above, allows us to construct a detailed model of the behavior of the atmospheric channel. We now have the tools necessary to characterize the atmospheric channel and the impact it has on different quantum protocols. Chapters 3 and 4 will be dedicated to the analysis of single-link and multi-link satellite-to-ground QKD scenarios respectively.

Chapter 3

Single-link satellite-to-ground QKD with adaptive optics

In order to determine the feasibility of the implementation of a satellite-to-ground quantum key distribution exchange aided by adaptive optics, we first start by examining the simplest case, a single link scenario. In the following we will give a brief look at the current state of the art, we will then detail the characteristics of the scenario considered, and the methodology employed for its simulation and finally, we will analyze the performance of such a system in terms of secret key rate [4].

3.1 State of the art

Quantum Key Distribution is one of the key research fields looking to secure communication exchanges beyond the mathematical or computational limitations of classical encryption systems. The technology involved in QKD systems has been actively developing over the last couple of decades but some limitations still remain. Most notably, the vast majority of experimental demonstrations have been performed through the use of optical fiber which significantly limits the distances at which a quantum exchange can be performed. Losses in fiber increase exponentially with distance and a lack of maturity in quantum repeater technology limits the implementation of QKD protocols to a few hundred kilometers [61–63]. It is possible to reach up to a thousand kilometers when employing QKD setups where additional intermediary nodes are needed such as with Twin-Field (TF) or Measurement Device Independent (MDI) protocols [64].

This limitation of terrestrial systems means that satellite-to-ground links present themselves as a promising alternative for the establishment of long-distance QKD links [65], useful for example in the context of an inter-continental quantum network. The attenuation of optical waves in free-space increases quadratically with distance, which has motivated several theoretical and experimental works in free-space QKD [59, 66–68]. Satellite QKD links have in particular been the subject of study due to the multiple additional challenges posed by the propagation of light through the atmospheric chan-

nel. Previous studies have focused on different atmospheric effects such as the beam wandering and broadening [3, 69, 70], the effect of pointing jitter and divergence [59, 66], and the Doppler effect [71] among others.

Another main effect of atmospheric propagation on light is the impact of turbulence on the spatial coherence of the signal. This aberration of the wavefront as explained in section 2, affects the coupling into the fiber, which is necessary for the use of coherent detectors for CV-QKD and SNSPDs for DV-QKD. Adaptive optics systems are already commonly used in astronomy applications [43, 53, 72]and more recently has become a key technology for the development of satellite optical telecommunications [53] and for free-space QKD [73–77].

Previous analytical works on AO-assisted satellite-to-ground QKD links [69, 73, 78] rely on simplified analytical models or make strong approximations like only accounting for the temporal error of the feedback loop or estimate an approximate performance through metrics like the Strehl ratio instead of analyzing the fiber coupling. One particular study [77] focuses on the analysis of finite Zernike modes while disregarding other AO limitations while other works perform numerical end-to-end simulations without taking into account fiber coupling [74, 79]. One of the most complete theoretical studies [75], does take into account end-to-end propagation as well as the effect of coupling into the fiber, however it considers a unique system design with set AO and ground station parameters and limits the performance estimation to a single DV protocol in the asymptotic regime.

Regarding experimental satellite-to-ground QKD demonstrations, the most notable one corresponds to the quantum exchange performed by the Micius satellite [80]. The Chinese Low Earth Orbit (LEO) satellite launched in 2016 has since performed several quantum-related experiments, including a downlink quantum exchange with a ground station employing the efficient decoy-state BB84 protocol. This is a significant achievement proving the feasibility of free-space-based quantum protocols over long distances (1200 km). However, operation was limited to nighttime and the signal was detected in free-space instead of directly being coupled into a fiber.

3.2 Scenario

The scenario we have chosen to consider can be found in figure 3.1. It involves a QKD link between Alice who is located onboard a LEO satellite and Bob who will be at a ground station. Alice will be located in an orbit between 400 km and 2000 km and will emit an optical beam of divergence θ_d in the direction of Bob. Her pointing is however not perfect, so the beam will move with respect to Bob's receiver aperture following a Gaussian probability distribution of mean 0 and standard deviation θ_p. The optical signal will propagate through the turbulent atmosphere before arriving to Bob's station

where it will be captured by a telescope of diameter D placed at height h_T with respect to the ground. Bob will be able to track Alice's satellite movement between 20° and 90° elevation with respect to the horizon, and he will be equipped with an adaptive optics system allowing him to partially correct the aberrations of the incoming wavefront. h_s corresponds to the altitude of the satellite orbit measured at the zenith. Since we assume a circular orbit, the distance from the ground station to the satellite at elevation ε is $R = h_s/\sin(\varepsilon)$.

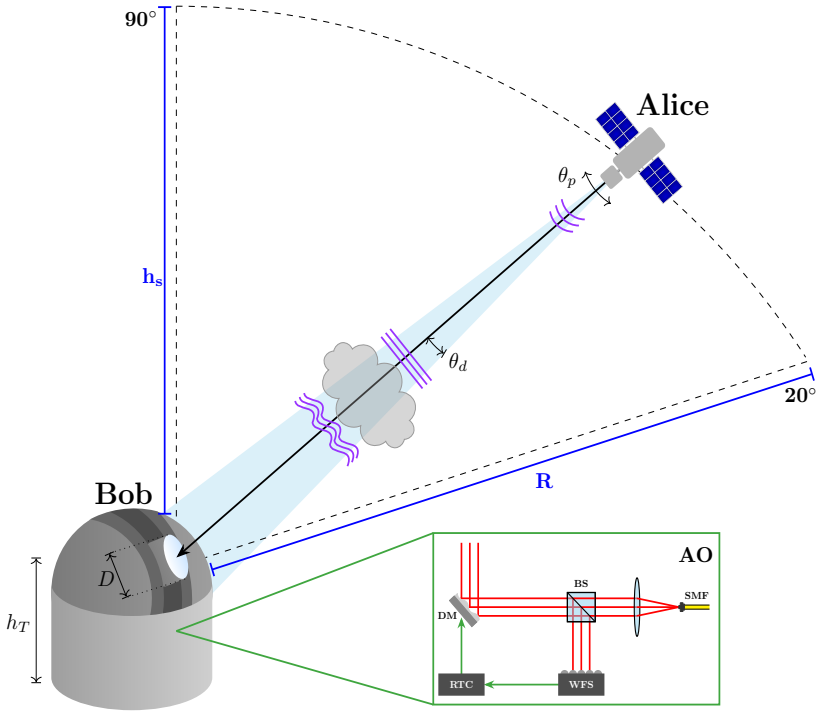


Figure 3.1: Quantum key distribution scenario between a LEO satellite and a ground station.

The limitation on the elevations being considered is due to limitations in state-of-the-art tracking and adaptive optics systems. In a practical implementation of such a system, a classical signal would have to be multiplexed along with the quantum signal in order to appropriately measure and correct the turbulence. Several QKD protocols already employ classical signals at a slightly different wavelength or in time intervals different from the quantum signal for synchronization purposes. For this study, we consider that classical signals we call pilots, are multiplexed in time with our quantum signal and will be sent at time intervals T_d.

For this first feasibility analysis we will consider both daytime and nighttime turbulence profiles of varying levels of severity. We consider as well different levels of adaptive optics correction described by the maximal number of Zernike radial orders the system

is able to correct. The performance metric we have decided to use in order to analyze the effect of turbulence on a QKD protocol is the final secret key rate, both in the asymptotic regime as a first approximation as well as in the finite-size regime to give a more realistic estimation. Finite-size effects are of particular significance in the case of LEO satellites since orbital dynamics mean that Alice will only remain visible by Bob for a few minutes.

We examine the estimated key rates for two fundamentally different protocols, one discrete variable and one continuous variable protocol, in order to see the effects of turbulence correction on both of them without necessarily taken a stance on which one is more advantageous. The aforementioned protocols are the *efficient two-decoy BB84* (DV-QKD) and the *Gaussian modulation* protocol (CV-QKD), both of which have been described in more detail in sections 1.2 and 1.3 respectively. For both protocols we consider some different noise levels, for the DV protocol it corresponds to different levels of background radiation while for CV it means different values of the excess noise.

3.2.1 Reference values

In the following we will describe the reference values for the main parameters involved in this simulation study. These parameters will either remain constant throughout or will serve as the baseline case of analysis. The parameters of the scenario that are common to the simulation of both protocols can be found in table 3.1. We have decided to consider the quantum exchange is performed at telecom wavelength and symbols are being sent at rate f_{TX}. The placement of the fiber with respect to the receiving aperture is assumed to respect the ratio (D/w_z) between the aperture diameter and the waist of the fiber mode at distance z, this ratio is optimized in order to maximize the coupling efficiency.

While the correction capacity of the AO system n_r is one of the characteristics that will vary in order to assess its effect, the rest of the AO system's parameters (feedback loop frequency, gain, etc.) remain constant throughout the study, these include the amount of Zernike radial orders in which the incoming wavefront is modelled to be projected n_{rmax} , the loop frequency f_{AO}, and the delay between the measurements and the actuator commands δ_t.

Parameter	Symbol	Value
Wavelength	λ	1550 nm
Pointing error	θ_p	1 μrad
Divergence	θ_d	10 μrad
Zenith transmittance	τ_{zen}	0.91
Transmission rate	f_{TX}	100 MSymbols/s
Receiver diameter	D	1.5 m
Receiver altitude	h_T	5 m
AO loop frequency	f_{AO}	5 kHz
AO loop frame delay	δ_t	2 frames
Wavefront projection	n_{rmax}	40 radial orders
Satellite altitude	h_s	400 km to 2000 km
Fiber/receiver ratio	D/w_z	2.2
Fixed attenuation	η_{opt}	2.8 dB

Table 3.1: General simulation parameters

The atmospheric transmittance due to absorption and scattering τ_{zen} has been obtained through the MODTRAN software [60] for wavelength λ in a mid-latitude summer atmospheric model with clear sky conditions corresponding to a 23 km visibility. We consider the satellite travels through a circular orbit, the satellite altitudes taken into account correspond to the range of LEO satellite altitudes and the divergence and pointing error of the beam are consistent with experimental results found in the literature [80]. The sampling frequency of the AO loop is of the same order of magnitude as the one from at least one ground station currently in development [81]. The fixed attenuation parameter η_{opt} is intended to account for all untrusted attenuation sources, atmospheric absorption, etc.

The baseline parameters specific to each one of the protocols can be found in tables 3.2 and 3.3, all of them were chosen in order to be consistent with values found in the literature for free-space QKD systems. In the case of DV, the detection efficiency η_d and the probability of erroneous detection e_d for example, are consistent with state of the art SNSPDs [66, 82], and the efficiency of error correction f_{EC} corresponds to standard error correcting codes [66]. In the case of CV, the chosen values are taken from a previous study of satellite-to-ground CV-QKD [3].

Parameter	Symbol	Value
Detection efficiency	η_d	0.85
Erroneous detection	e_d	0.01
Z basis probability	q	1
Temporal window	Δt	500 ps
Correctness parameter	ε_{corr}	10^{-10}
Security parameter	ε_{sec}	10^{-10}
Error correction efficiency	f_{EC}	1.16

Table 3.2: Simulation parameters for the efficient two-decoy BB84

Parameter	Symbol	Value
Detection efficiency	η_d	0.4
Electronic noise	ν_{el}	10% SNU
Pilot energy	E_{ref}	10 pJ
Pilot period	T_d	1 ns
Pilot bandwidth	$\Delta\nu_{ref}$	10 kHz
Reconciliation efficiency	β	0.95
Fixed excess noise	ξ_{fix}	1-5% SNU

Table 3.3: Simulation parameters for the Gaussian modulation protocol

Noise considerations

The performance of both protocols will be analyzed for a couple different noise levels in order to have a more general idea of the conditions under which their implementation is feasible. The key noise parameter for discrete variable corresponds to the background noise and for continuous variable it is the excess noise of the system, we present here the noise analysis we have decided to employ.

- **Background noise Y_0 (DV-QKD):**

  The background noise or 0-photon yield is defined as the probability of Bob detecting a photon when Alice has not sent one. The main contributing factors to this yield are the detector's dark counts and the background photons that are scattered in the atmosphere and end up inside the fiber's field-of-view. We have chosen to take into account two noise scenarios, a pessimistic case in which an illuminated satellite reflects sunlight into the receiver, and a more realistic case of average daytime or nighttime background radiation.

  For the pessimistic case we find a photon background rate N_b measured during one passage of a GLONASS satellite [83] in which its solar panels were directly

reflecting solar radiation into a 1.5 m receiver telescope, resulting in a measured rate of $N_b = 1.9 \cdot 10^3$ photons/s. However, the GLONASS constellation is at an altitude of around 20000 km and the measurements were done at a 532 nm wavelength. After accounting for this as well as the different width of the interference filters (3 nm for GLONASS and 0.8 nm considered in our study), we obtain an equivalent rate of $N_b = 1.6 \cdot 10^5$ photons/s. This rate is significantly larger than the dark count rate of the detectors considered which is of the order of ≈ 200 photons/s, the dark count can thus be neglected. If we then approximate the background noise as $Y_0 = N_b \Delta t$ and considering a temporal detection window of $\Delta t = 500$ ps, we obtain a pessimistic yield of $Y_0 = 8.1 \cdot 10^{-5}$. This will be the worst case scenario considered for both day and night.

For the daytime background noise we estimated the sky radiance through the computer code LOWTRAN [84], a low-resolution propagation model that takes into account different atmospheric conditions and aerosol models in order to estimate the sky radiance and atmospheric transmission at a specific wavelength. Considering a rural environment with clear sky, a 23 km visibility and a 45° solar angle, the sky radiance computed by LOWTRAN is appropriately $H_b \approx 5 W m^{-2} \mu m^{-1} sr^{-1}$. This allows us to calculate the photon background rate as:

$$N_b = \frac{H_b \Omega_{FOV} A_{RX} B_{filter} \lambda}{hc} \eta_{opt} \eta_d \tag{3.2.1}$$

H_b is the aforementioned sky radiance, h the Planck constant, c the speed of light, A_{RX} the area of the receiver telescope (1.77 m^2 in our case), $B_{filter} = 0.8$ nm is the bandwidth of the optical interference filter and Ω_{FOV} is the field-of-view of the receiver. Given that the receiving telescope is located at a distance from a single-mode fiber such that the coupling is optimal [52], the field-of-view can be estimated through the following equation [85]:

$$\Omega_{FOV} = \pi \left(0.713 \frac{\lambda}{D} \right)^2 \tag{3.2.2}$$

The field-of-view of our receiver with diameter $D = 1.5$ m, corresponds to $1.71 \cdot 10^{-12}$ sr which results in a background rate of $N_b = 4.2 \cdot 10^4$ photons/s. That gives us a less pessimistic estimation for the daylight background noise of $Y_0 = 2.1 \cdot 10^{-5}$.

For the nighttime background noise we consider the sky background radiance becomes negligible, meaning that the 0-photon yield will be determined by the dark counts of the detector $N_b = 200$ photons/s, which corresponds then to a background noise of $Y_0 = 1 \cdot 10^{-7}$.

- **Excess noise ξ (CV-QKD):**

  The excess noise of the CV-QKD system at hand will come from four main contributions: $\xi = \xi_{fix} + \xi_{fad} + \xi_{pn} + \xi_{tp}$. The fixed excess noise ξ_{fix} is intrinsic to the system and usually caused by experimental imperfections, for our study we will consider fixed excess noise values of 1, 3 and 5 % SNU. The fading excess noise ξ_{fad} corresponds to the additional noise due to the fading nature of the atmospheric channel and can be modelled as such:

  $$\xi_{fad} = \frac{Var(T)}{E[T]^2} V_A \tag{3.2.3}$$

  ξ_{fad} will thus depend on the variance and mean value of the transmission coefficient of the channel T, as well as the variance of Alice's symbols V_A.

  The last two contributions are related to the pilot signals and the phase recovery scheme [86]. ξ_{pn} is due to the fact that the phase recovery process will be affected by the shot noise, which introduces an excess noise that can be estimated as:

  $$\xi_{pn} = \frac{V_A E_{ph}}{2\eta_d E_{ref} T^2} \tag{3.2.4}$$

  This noise is then dependent on the energy of a photon E_{ph} as well as the energy of the reference pilot signal E_{ref}. The last contribution to the excess noise considered ξ_{tp} is due to the time elapsed between reference signals T_d. We can estimate it as: $\xi_{tp} = V_A 2\pi T_d \Delta\nu_{ref}$ where $\Delta\nu_{ref}$ corresponds to the linewidth of the laser used for the pilot signal.

3.3 Simulation

The procedure we follow in order to simulate the performance of the satellite-to-ground QKD link is illustrated in figure 3.2. It consists of five simulation stages. The first stage, **turbulence modelling**, involves the construction of atmospheric turbulence profiles from experimental measurements as explained in section 2.1.1. The second stage, **AO simulation**, will estimate the effect of the atmospheric profile from stage one on the optical signal. The coupling efficiency for a specific set of AO parameters and satellite orbit is calculated. This is done through the simulation tool SAOST introduced in section 2.2.4.

Stage three, the **pointing jitter simulation**, is done in parallel from stage two because we consider the effects of beam wandering and atmospheric turbulence to be independent of one another. This hypothesis of independent behavior was validated by modifying the original SAOST simulator as will be explained further on. This stage

takes into account the path losses and the losses due to the divergence and wandering of the beam. The previous steps are computed for a specific elevation angle. In stage four, **trajectory statistics**, after the previous stages have been performed for all the elevations considered, they are combined in order to obtain the probability distribution of the transmission efficiency (PDTE) for an entire satellite pass. In the last stage, **key rate estimation**, the performance of the system is calculated through the secret key rate of each protocol.

The details of each stage as well as the intermediary results obtained will be explained in the following.

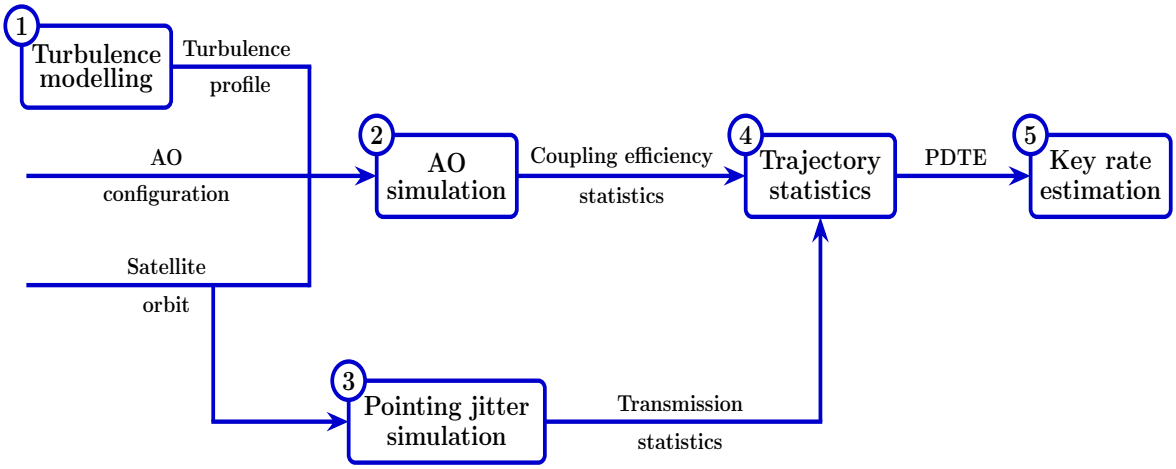


Figure 3.2: Structure of the simulation process.

3.3.1 Turbulence modelling

In order to assess the feasibility of a quantum exchange through an atmospheric channel we first need to establish the turbulence conditions we want to consider and construct a turbulence profile accordingly. In the interest of maximizing communication with the satellite we consider both daytime and nighttime operation and following the process described in 2.1.1, we were able to create four profiles for each operation regime. The profiles will be labeled D_i for daytime and N_i for nighttime for i between 0 and 3, corresponding to turbulence conditions of increasing severity.

Different turbulence strengths will correspond to different thresholds for the r_0 and θ_0 parameters. The parameter thresholds are chosen from the inverse cumulative probability distribution of the available data. For example, if we wish to represent mild turbulence conditions from our dataset, we may choose a Fried parameter r_0^i such that $P(x > r_0^i) = 20\%$, meaning that only 20% of the values from our dataset correspond to an r_0 higher than the one we chose, or in other words, 80% of the time we will encounter turbulence conditions worse than the ones represented by the r_0^i selected.

The probabilities of occurrence of the four types of profiles created (D_0 to D_3 and N_0 to N_3) are: $P(x > r_0^0) = 20\%, P(x > r_0^1) = 50\%, P(x > r_0^2) = 75\%$, and $P(x > r_0^3) = 95\%$. Since we consider only LEO satellites in this study, the isoplanatic angle θ_0 of the profile is relevant for the estimation of the correlation time τ_0. In the interest of coherence we have chosen the thresholds for both parameters of interest to be $P(x > \theta_0^i) = P(x > r_0^i)$.

The four daytime and nighttime profiles we constructed are illustrated in figures 3.3 and 3.4 respectively, the corresponding tables contain the values of the integrated parameters at the zenith for each of the profiles.

	$\mathbf{D_0}$	$\mathbf{D_1}$	$\mathbf{D_2}$	$\mathbf{D_3}$
$\mathbf{r_0}$ (cm)	24.8	15	10.6	6.9
$\theta_\mathbf{0}$ (μrad)	45.8	34.5	25.8	18.1
$\tau_\mathbf{0}$ (ms)	1.97	1.43	1.10	0.77
$\sigma_\chi^\mathbf{2}$	0.005	0.01	0.01	0.02

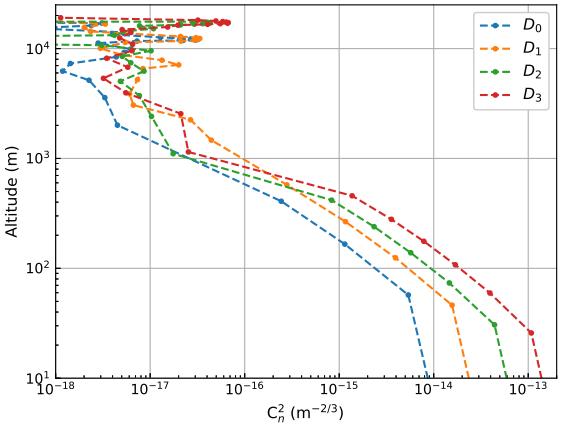


Figure 3.3: Daytime turbulence profiles and corresponding integrated parameters

	$\mathbf{N_0}$	$\mathbf{N_1}$	$\mathbf{N_2}$	$\mathbf{N_3}$
$\mathbf{r_0}$ (cm)	68.6	50.4	37.8	22.9
$\theta_\mathbf{0}$ (μrad)	45.9	34.4	25.9	18.1
$\tau_\mathbf{0}$ (ms)	2.09	1.56	1.22	0.86
$\sigma_\chi^\mathbf{2}$	0.0045	0.008	0.01	0.02

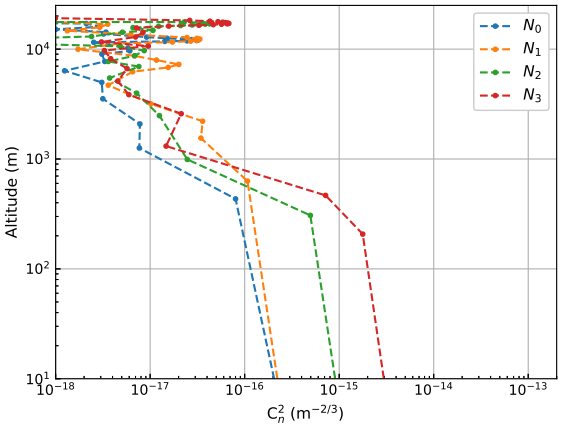


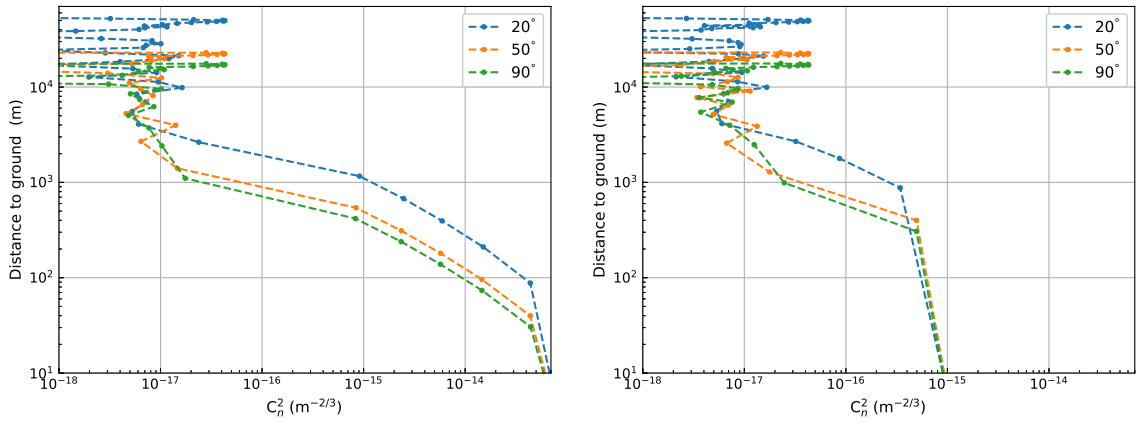
Figure 3.4: Nighttime turbulence profiles and corresponding integrated parameters

As we can see, each profile consists of around 20 C_n^2 values at different altitudes, with generally low values at altitudes above 1 km. The behavior of the refractive index constant is very variable throughout the upper layers of the atmosphere while for lower altitudes the evolution is smoother. The values from the upper layers of the atmosphere for daytime and nighttime come from the same set of data, measurements taken at Cerro Paranal in Chile. Since θ_0 is mostly dependent on those high layers, we obtain very similar isoplanatic angles for day and night profiles.

The Fried parameter on the other hand, varies considerably between profiles and is significantly higher for nighttime conditions which is coherent with the fact that turbulence effects can be heightened by solar irradiance. The scintillation index estimated for our different turbulence conditions is consistent with us working on the weak perturbation regime, the highest value being $\sigma_\chi^2 = 0.02 < 0.3$. The coherence time of the turbulence is of the order of one to two milliseconds for all eight profiles, with slightly higher values for the night profiles, and was calculated through equation 2.1.4.

The effect of all eight turbulence profiles on the optical signal and thus the performance of the key rate will be analyzed further on. However, we have decided to choose two main profiles D_2 and N_2 to serve as our baseline turbulence conditions. We have chosen this specific profiles in order to evaluate the feasibility of the QKD link under a reasonably strong but not overly pessimistic turbulence scenario.

In figure 3.5, we can observe each of the baseline profiles adjusted to account for different elevations.



(a) Daytime (b) Nighttime

Figure 3.5: Turbulence profiles for different elevations of our baseline turbulence conditions

As we can see, observing the satellite from any elevation lower than 90° will elongate the path along which the optical signal will have to propagate. This means that longer

stretches of the propagation trajectory will be spent at low altitudes where turbulence is stronger, which as can be interpreted from the integrated parameters in table 3.4, results in the signal experiencing worse turbulence conditions overall.

	$\mathbf{D_2}$		$\mathbf{N_2}$	
Elevation	**20°**	**90°**	**20°**	**90°**
$\mathbf{r_0}$ (cm)	5.6	10.6	19.9	37.8
$\theta_\mathbf{0}$ (μrad)	4.7	25.8	4.7	25.9
$\tau_\mathbf{0}$ (ms)	0.91	1.1	1.15	1.22
$\sigma_\chi^\mathbf{2}$	0.09	0.01	0.07	0.01

Table 3.4: Integrated parameters for the baseline profiles at 20° and 90° elevation

3.3.2 Adaptive optics simulation

With our turbulence profiles having been constructed we can now estimate their effect on the coupling efficiency and how an adaptive optics system may be able to mitigate some of it. This will be done with the help of the simulation tool SAOST explained in section 2.2.4. Each simulation is done for a given set of the following parameters: satellite altitude, turbulence profile, radial orders corrected by the AO system and elevation, for which an error budget is derived. Table 3.5 shows an example of the decomposition of the error budget for our baseline daytime turbulence conditions for two different AO correction capabilities.

	$\mathbf{n_r = 5}$		$\mathbf{n_r = 20}$	
Elevation	**20°**	**90°**	**20°**	**90°**
σ^2_ϕ (rad^2)	249.09	85.23	249.09	85.23
σ^2_{fit} (rad^2)	4.87	1.66	0.44	0.15
σ^2_{alias} (rad^2)	1.70	0.58	0.16	0.05
σ^2_{tempo} (rad^2)	0.06	0.06	0.14	0.11
σ^2_{res} (rad^2)	6.63	2.31	0.74	0.32

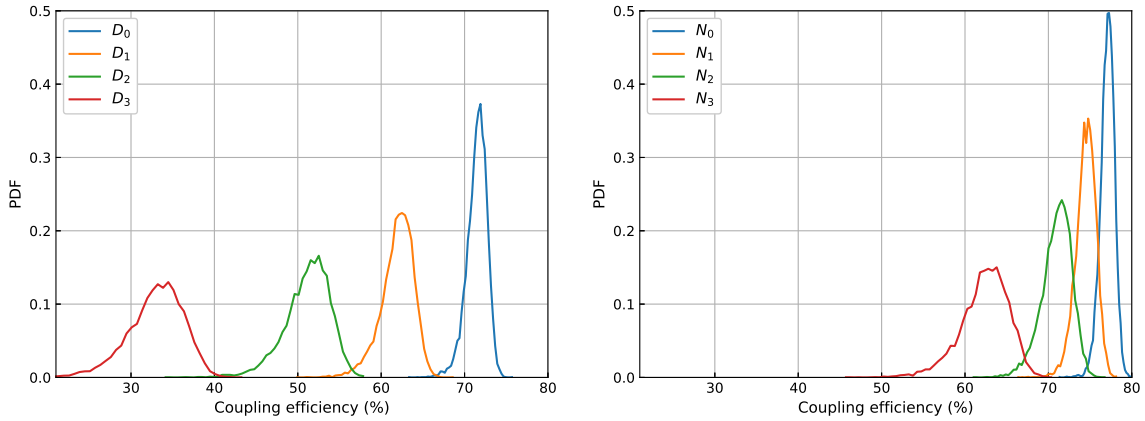
Table 3.5: Error budget for a D_2 turbulence profile and a satellite altitude of 400 km

σ^2_ϕ corresponds to the spatial variance of the phase of the optical signal after propagation through the specific turbulence condition described by the profile. As we can see it is considerably larger for low elevations. σ^2_{fit}, σ^2_{alias} and σ^2_{tempo} are the main contributions to the residual phase variance after AO correction σ^2_{res}. Since we have chosen to consider a relatively high sampling frequency for the AO loop (5 kHz), the temporal error has the lowest impact on the total residual phase. This is why in our study we have decided to focus on the effect of the number of corrected radial orders n_r, which will mainly affect the fitting error, the biggest contributor to the total error. It should be noted that a better AO correction i.e. a bigger n_r, will significantly reduce the fitting

and aliasing errors while slightly increasing the temporal error of the system.

For every simulation, 10000 occurrences are generated characterized by the variances described in the error budget and the coupling into the fiber is calculated for each one of them. From this, it is possible to derive the statistical behavior of the coupling for a given set of conditions. In the following, we will analyze how varying the four core parameters of our simulation: turbulence strength, corrected orders, elevation and satellite altitude, will impact the probability distribution of the coupling efficiency.

Figure 3.6 shows the coupling efficiency for the eight different turbulence profiles generated during the last stage. This was done for a 400 km altitude satellite at the zenith and considering an AO capable of correcting 15 radial orders.

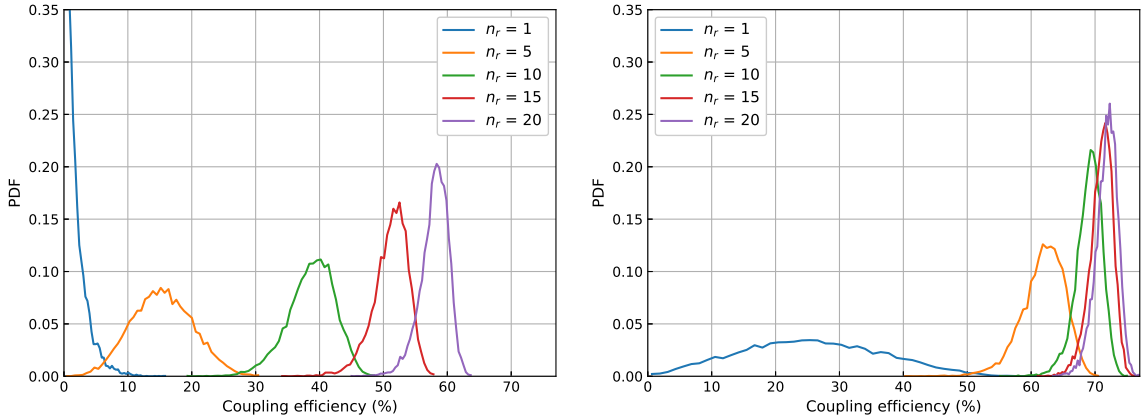


(a) Daytime (b) Nighttime

Figure 3.6: Probability distribution of the coupling efficiency for different turbulence profiles. ($\varepsilon = 90°$, $h = 400$ km, $n_r = 15$)

As can be predicted, the profiles representing milder turbulence conditions result in higher average coupling efficiencies, as well as a reduced standard deviation as evidenced by the narrowing of the distributions. The daytime turbulence profiles cover a larger range of coupling efficiency values. In contrast, for nighttime the mean values are closer together, accumulating closer to the theoretical maximum of 81% coupling of a Gaussian beam into a circular aperture [52]. This accumulation of nighttime values is due to the weaker turbulence conditions represented and the high level of AO correction considered.

Figure 3.7 illustrates the coupling efficiency for all 5 different levels of AO correction taken into account. We still consider a 400 km orbit and 90° elevation, but this time we focus on our reference profiles D_2 and N_2.



(a) Daytime

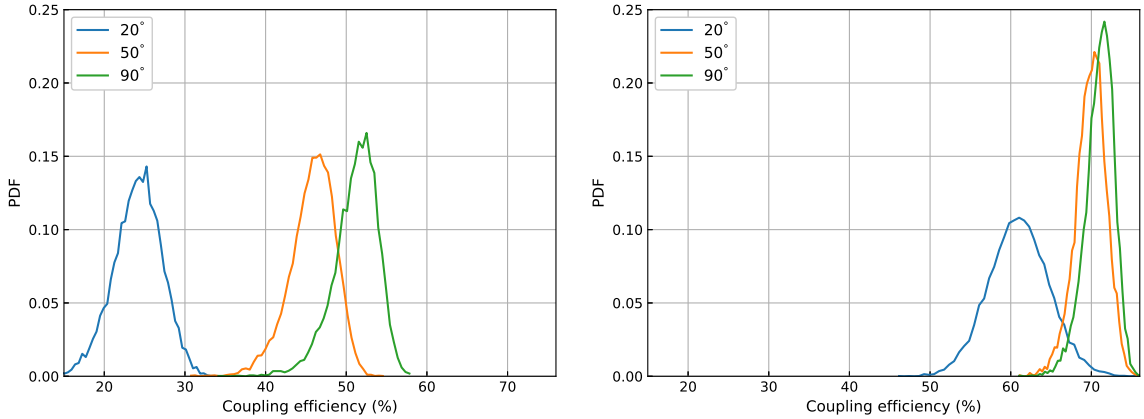
(b) Nighttime

Figure 3.7: Probability distribution of the coupling efficiency for different number of corrected orders. ($\varepsilon = 90°$, $h = 400$ km, D_2 and N_2 profiles)

We can observe that as anticipated, the correction of more radial orders leads to better coupling into the fiber both in terms of average and variance of the distribution. It is interesting to note that while most of the probability distributions pictured resemble a Gaussian distribution (and can in fact be approximated to one), a more extreme case, such as the day profile with only tip-tilt correction ($n_r = 1$) is more comparable to an exponential probability distribution. Moreover, for the night profile the coupling efficiency seems to be reaching something akin to a saturation limit. With the night turbulence represented already not being very strong, increasing correction from 10 to 15 and 20 radial orders does not have as much of a significant effect as it does for the daytime conditions.

In figure 3.8 we can see how the coupling efficiency changes for three different elevations. For this, we assume a 400 km satellite orbit, our reference profiles D_2 and N_2 and correction of 15 radial orders.

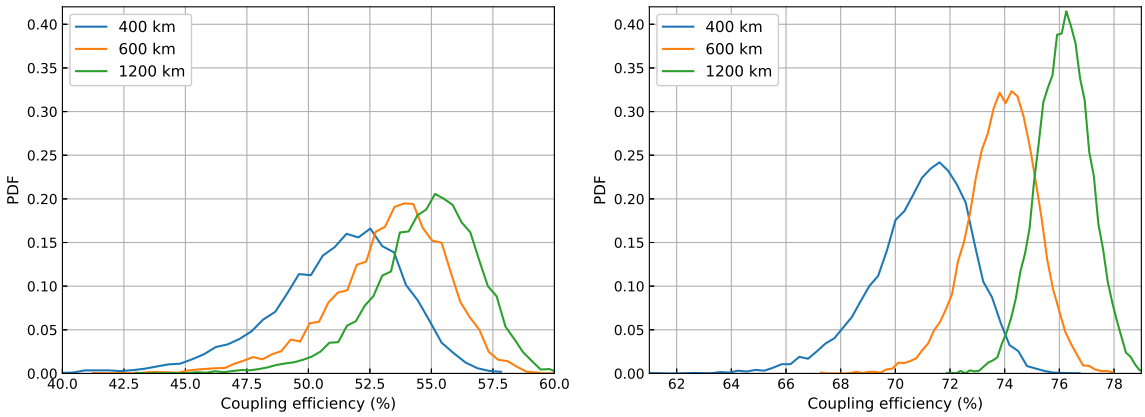
Coupling efficiency will be greatly decreased for the same turbulence conditions when communicating with the satellite at a lower elevation due to a longer propagation distance on the more turbulent lower layers of the atmosphere. The dependence of coupling on elevation is however not linear. The coupling efficiency at 20° differs significantly from the coupling at 50°, while the difference between this last one and the efficiency at 90° is not as notable. This is in part due to the fact that the path length dependence on elevation is not linear either, and also in part due to the fact that elevation influences multiple parameters involved in the simulation like the turbulence conditions and the apparent wind speed for example.



(a) Daytime (b) Nighttime

Figure 3.8: Probability distribution of the coupling efficiency for different elevations. ($n_r = 15$, $h = 400$ km, D_2 and N_2 profiles)

Finally, in figure 3.9 we can see the effect of different satellite altitudes on the coupling efficiency. This was done for a 90° elevation, our baseline D_2 and N_2 profiles and considering an AO capable of correcting 15 radial orders.



(a) Daytime (b) Nighttime

Figure 3.9: Probability distribution of the coupling efficiency for different satellite altitudes. ($\varepsilon = 90°$, $n_r = 15$, D_2 and N_2 profiles)

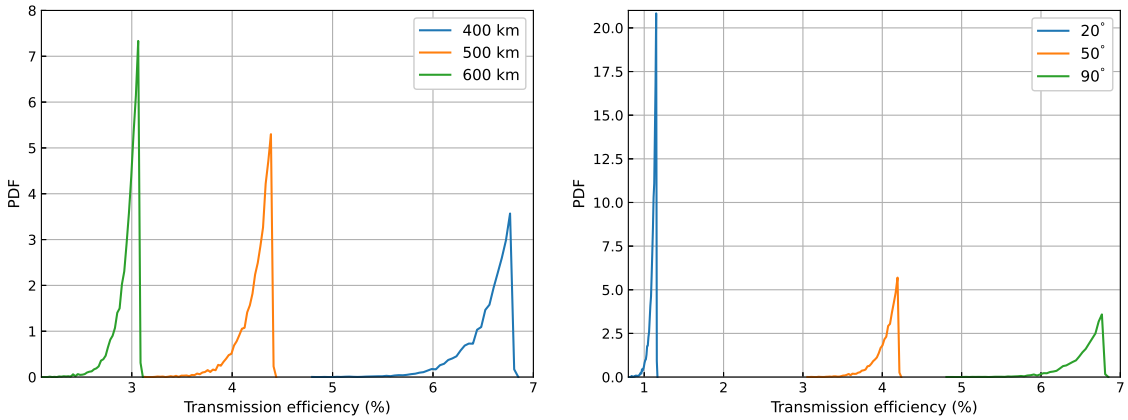
Since this simulation stage does not take into account the path loss, the effect of satellite altitude on the coupling is different from what would be expected at first glance, with all three distributions not differing that much from one another. We consider the same elevation in all three cases, meaning that the turbulence traversed by the optical

signal is identical in all three cases. What changes is in fact the wind profile. As explained earlier on, the wind profile for an optical link with a LEO satellite includes a contribution due to the displacement of the satellite across the sky. This contribution is directly proportional to the satellite speed $V_{sat} = \sqrt{GM_T/R}$ and inversely proportional to the distance R to the satellite. This explains why we obtain better coupling efficiencies for higher satellite altitudes, less wind results in a higher coherence time and thus a lower temporal error.

3.3.3 Pointing jitter simulation

The third stage of simulation is performed separately from the first and second stages. This simulation does not include the effects of turbulence, it will only take into account the so-called path loss or geometrical loss, and the effects of beam wandering due to the pointing error of the satellite.

This is done through numerical simulations following the equations shown in section 2.3.1. A simulation is performed for each specific satellite altitude and elevation angle. Each run consists of 10000 random occurrences of deflection distances consistent with the Weibull style probability distribution presented in equation 2.3.5, with mean zero and a standard deviation dependent on the pointing error of the satellite. Then, the transmission efficiency corresponding to each distance from the center of the aperture, is calculated through equation 2.3.7. From the resulting values of T^2, it is then possible to derive the probability distribution of the transmission due to beam wandering. Figure 3.10 shows some examples of the resulting distributions obtained.



(a) Altitude (b) Elevation

Figure 3.10: Probability distribution of the transmission efficiency for different satellite altitudes at 90° elevation and different elevations of a satellite at $h = 400$ km

The first notable remark about these distributions is the fact that the transmission

values are very low, of the order of a few percentage points. This already indicates that this part of the total transmission efficiency estimation will contribute greatly to the final losses of the channel. In addition to that, we can observe that the distributions obtained appear to display an almost exponential increase and then drop abruptly to 0. The percentage of light captured by the aperture, increases the shorter the deflection distance is, since it means less light is being lost outside the receiver. Therefore, the maximum achievable efficiency corresponds to a deflection distance equal to zero, when the beam is perfectly centered into the receiving aperture.

Because this simulation stage does not take into account the effects of turbulence, the difference of performance of the scenarios pictured above is mainly dictated by distance. Distance to the satellite is going to determine the widening of the incoming beam, with a larger beam (compared to the dimension of the receiving aperture), meaning a lower proportion of the received light can actually be captured by the ground station telescope. The effect of different propagation distances can be clearly seen in figure 3.10a where when observed at the zenith, the transmission efficiency of satellites at different altitudes varies significantly, with greater distances producing a narrower distribution with much lower values. This can be similarly be observed on figure 3.10b, in this case, a single satellite altitude is considered (400 km), and the transmission was simulated for different elevations. The higher losses at lower elevations are mainly due to the longer path the light has to travel through which results in a widened beam and therefore more losses.

3.3.4 Trajectory statistics

Once the coupling efficiency and pointing jitter simulations have been performed for every elevation within the range considered in this scenario, the next step is to combine them into a probability distribution of the transmission efficiency (PDTE), representative of an entire satellite pass.

Under the hypothesis that the effects of turbulence and beam wandering are independent form one another, the total transmission efficiency at any given point of the trajectory can be described as:

$$\tau = T^2 = \eta_{ce}\eta_{bw}\tau_{atm} \tag{3.3.1}$$

Where η_{ce} is the coupling efficiency from the adaptive optics simulation, η_{bw} is the transmission efficiency from the pointing jitter simulation and τ_{atm} the transmission efficiency factor due to absorption and scattering calculated through equation 2.3.10 with the help of the MODTRAN tool. τ_{atm} is a constant value for each elevation considered but (under our hypothesis) η_{ce} and η_{bw} are independent random variables following the probability distributions that have been described in the previous steps. Thus, the probability distribution of the total transmission efficiency for a certain elevation ε is

calculated as:

$$PDTE_{\varepsilon}(\tau) = \tau_{atm} \int_{-\infty}^{\infty} P_{AO}(x) P_{BW}(\tau/x) \frac{1}{|x|} dx \tag{3.3.2}$$

$P_{AO}(x)$ and $P_{BW}(x)$ are the probability distributions corresponding to η_{ce} and η_{bw} respectively.

Nevertheless, this statistical description of the atmospheric channel's behavior hinges on the assumption that $P_{AO}(x)$ and $P_{BW}(x)$ are completely independent of each other. Thus, before moving on with the next stage of our simulation process, we decided to validate this hypothesis. In order to do that, we decided to compare the results of using equation 3.3.2 to estimate the final probability distribution at a given elevation with a modified version of our turbulence simulator SAOST.

SAOST in its original version only computes the overlap integral between the aberrated wave captured by the reception pupil and the mode of a single mode fiber, in other words the resulting efficiency is normalized by the *power in the bucket*. It does not take into account the propagation losses nor the proportion of the wave that is indeed captured by the receiving aperture. In addition to that, it works under the hypothesis that the amplitude of the wave is constant upon reception and neglects the effects of scintillation. In order to remove the limitations involved by these premises, the code was modified to more accurately represent our study case in what we will call SAOST++.

First of all, the propagation of the field is now simulated via a Fourier transform approximation. The transmission pupil is assumed to be uniformly illuminated which results in an Airy disk at reception. The equivalent transmission pupil diameter that better approximates the Gaussian beam propagation from the pointing jitter simulations, can be calculated as $D_{Tx} = \sqrt{8}\lambda/(\pi\theta_d)$. A Fourier transform is then applied to the full transmission disk, resulting in the aforementioned Airy pattern that will be collected by the receiver pupil. Finally, in order to estimate the coupling efficiency an overlap integral is computed between this received Airy disk and the mode of a single mode fiber.

These modifications of the simulation tool now permit the inclusion of the effects modelled by Vasylyev in [59]. On one hand, an estimation of the diameter of the main lobe of the Airy disk as $0.43\lambda L/\omega_0$ [87] with ω_0 the beam waist at the transmitter and L the propagation distance, allows for a proportionate dimensioning of the reception pupil within the simulation which accounts for the geometrical losses of the wave. On the other hand, it is now possible to emulate the pointing jitter of the satellite by displacing the uniformly illuminated transmitter before propagation, assuming a certain angular pointing error standard deviation and a normal distribution centered around zero. In this new SAOST++, for each iteration of the system, a random displacement

will be applied on the emitted beam and propagation is emulated via Fourier transform. Spatial phase aberrations and scintillation effects are estimated from an error budget as with the original SAOST and are then applied to the received Airy pattern cropped by the ground pupil. Coupling efficiency is estimated and after numerous iterations we obtain either a temporal series or a statistical distribution of transmission efficiency coefficients.

We verified that SAOST++ produced results coherent with what would derive from equation 3.3.2. As seen in figure 3.11 both approaches are equivalent from a statistical point of view but the modified SAOST tool allows for the integration of all the considered effects in a single simulation.

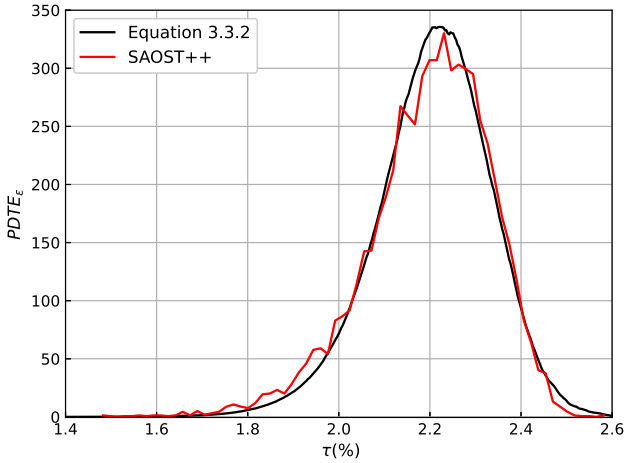
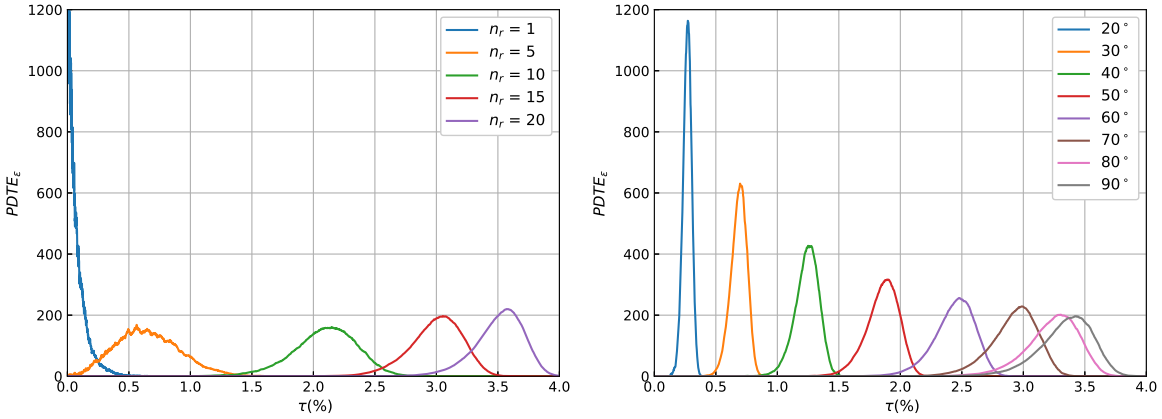


Figure 3.11: Comparison of the transmission efficiency of the analytical equation and the modified SAOST++. Turbulence profile D_2, 500 km satellite altitude and 80° elevation.

Having corroborated the validity of the hypothesis of the independence of turbulence effects and beam wandering, we proceed to employ equation 3.3.2 for the remainder of our simulation study.

Figure 3.12a illustrates some examples of how the distribution of the product $PDTE_\varepsilon$ looks. This was estimated for all the AO correction levels considered as well as several elevations. The general form of the distributions resembles the original $P_{AO}(x)$ while the much lower mean values reflect the influence of the $P_{BW}(x)$ distribution.



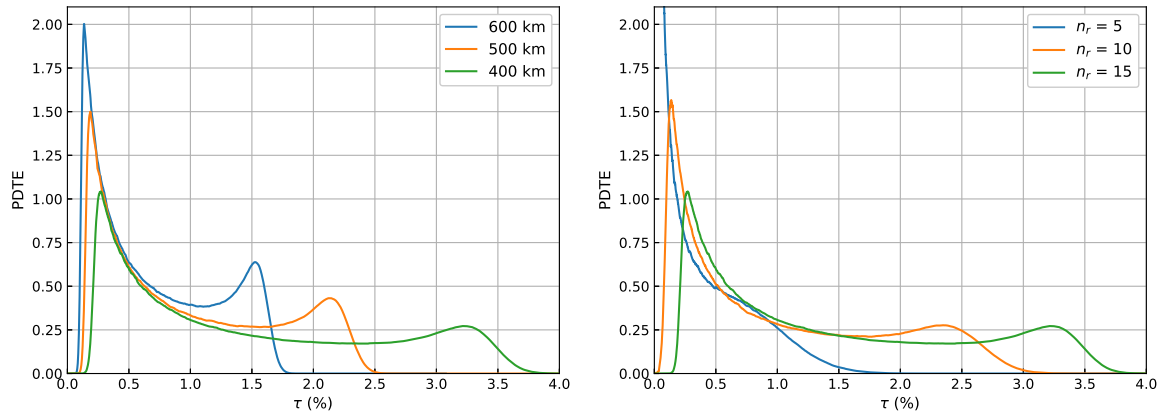
(a) Impact of AO correction

(b) Impact of elevation

Figure 3.12: $PDTE_\varepsilon$ for different AO correction at 50 ° elevation and for different elevations with an AO correcting 15 radial orders. $h = 400$ km

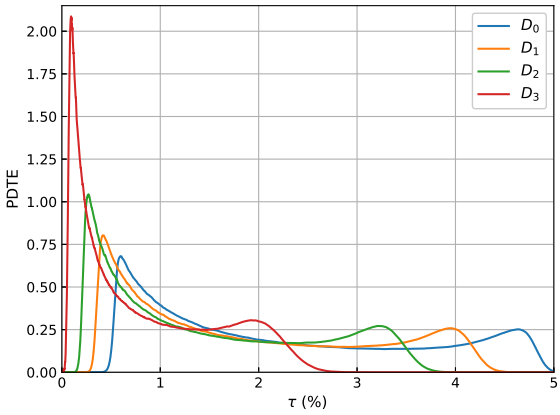
With the $PDTE_\varepsilon$ having been computed for every elevation, we can then calculate the total probability distribution for an entire satellite pass by adding the distributions of all the elevations considered. We discretized the orbit in approximately 100 intervals.

Figure 3.13 shows several examples of the resulting probability distributions. Here, we can see how variations in satellite altitude, AO correction and turbulence strength can affect the overall efficiency of the atmospheric channel.



(a) Impact of altitude

(b) Impact of AO correction



(c) Impact of turbulence conditions

Figure 3.13: Probability distribution of the transmission efficiency for an entire satellite pass. (a) Different satellite altitudes, $n_r = 15$, D_2. (b) Different AO correction, $h = 400$ km, D_2. (c) Different turbulence profiles, $n_r = 15$, $h = 400$ km

As we can see, the PDTE for an entire satellite pass has a very particular shape, it presents two noticeable peaks near the minimum and maximum values of τ and there is gap in the distribution for the values around zero. The gap is due to the fact that we do not consider elevations below 20° so, except in the case of very low AO correction, we will not encounter a scenario where the transmission efficiency is likely to be zero. The two peaks in probability can be explained by observing how the $PDTE_\varepsilon$ behaves for different elevations, as shown in figure 3.12b. The probability distributions at low elevations are very narrow, with significantly high probability of resulting in a low τ value, which produces the first prominent peak of the final $PDTE$. In contrast, for high elevations, the distributions are wider with a higher standard deviation, however, the distributions start overlapping once we get closer to the zenith which when adding all the $PDTE_\varepsilon$ results in the second much less prominent peak towards the highest possible values of our PDTE. This is consistent with results obtained previous to our study in [3] which employs a similar methodology to compose the $PDTE$ over a satellite pass but consider the AO effect to be constant.

It should be noted that the PDTE of the scenarios where low AO correction was considered (typically $n_r = 1$ or $n_r = 5$), turbulence effects remain strong and the distribution does not follow the same shape as described above. Instead, they present a maximum in the probability around a transmission efficiency equal to zero, followed by a pseudo-exponential decrease. The reason for this, as can be seen in figure 3.12a, is that distributions for lower AO correction are predictably concentrated around very low or zero τ values, showing an exponential decrease for lower elevations.

The effects of satellite altitude on the final PDTE can be observed in figure 3.13a. As

expected, at lower altitudes higher values of the transmission efficiency can be reached because of the reduced distance to the satellite and thus lower path loss. However, the distribution encompasses a wider range of values of τ, resulting in a higher variance. This could be a problem for the CV protocol since an increased variance will induce a higher fading excess noise. Figures 3.13b and 3.13c show the effect of AO correction and turbulence strength on the final PDTE. The number of corrected orders will determine the general form of the distribution, with higher correction ensuring higher transmission efficiencies can be achieved, as well as an important reduction in the probability of a low τ. Regarding the turbulence strength, the PDTE behaves as expected, with harsher turbulence conditions producing distributions concentrated around very low transmission efficiency values while a more benevolent turbulence scenario covers a wider range of τ values centered around slightly higher efficiencies.

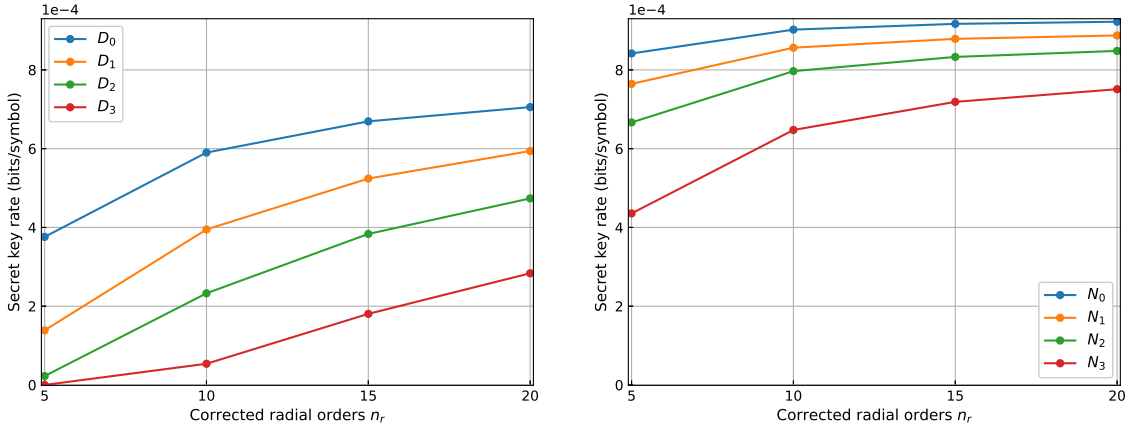
3.4 Key rate estimation results

Performing all the preceding stages of simulation allows us to model the propagation channel via the PDTE. We now have an estimation of the statistical behavior of the channel for each combination of satellite altitude, AO correction and turbulence strength, which will allow us to determine how a QKD system would perform under those circumstances. In the following, we study how variations of some system parameters affect the performance of the two studied protocols and which conditions would favor the feasibility of a satellite-to-ground implementation.

The way we compute the key rate is by applying the equations for each protocol (detailed in section 1) to all the possible values of the transmission efficiency τ for a given channel, and then with the help of the PDTE, we calculate the expected value of the key rate both in the asymptotic regime and taking into account finite-size effects. For the latter, we assume that the source is able to generate symbols at a rate of 100 Mhz, with each symbol being a photon or a coherent state for the DV and CV protocols respectively.

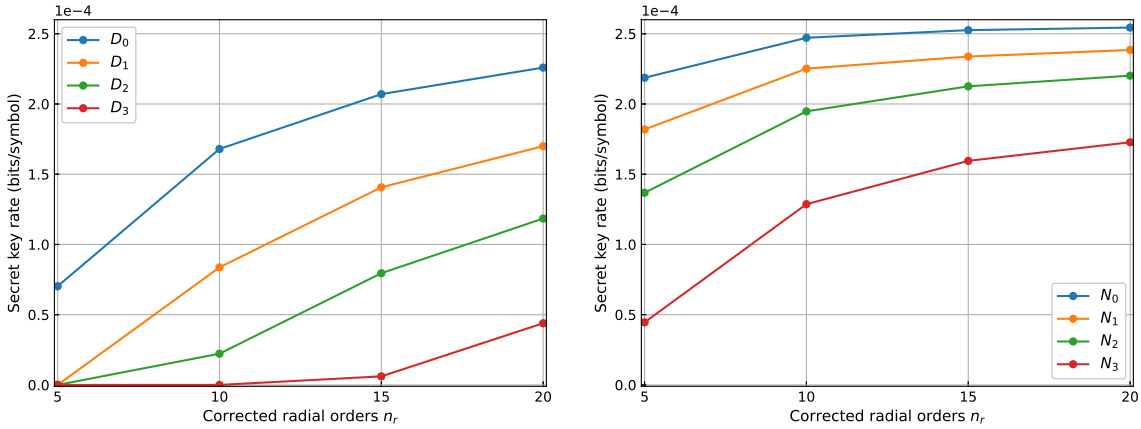
There is an optimization process involved in the key rate estimations for the protocols. For CV, the variance of Alice's symbols V_A is varied until the value resulting in the higher key rate is found. For the DV protocol, the best value of the key rate is found by optimizing over five parameters: the probability of choosing the Z basis q, the mean number of photons per pulse of the signal μ and of the weak decoy ν, and their respective probabilities of occurrence p_μ and p_ν respectively. For both protocols, the PDTE is divided into different intervals in order to reduce the effects of fading and the amount of divisions is optimized as well. More divisions result in a lower variance of that section of the PDTE but ultimately reduce the number of symbols as well, worsening finite-size effects.

The first thing we examined was how the different levels of complexity of the AO system considered, would affect the secret key rate performance in different turbulence conditions.



(a) Daytime (b) Nighttime

Figure 3.14: Finite-size secret key rate of the DV-QKD protocol for different AO corrections at $h = 500$ km. $Y_0 = 2.1\text{e-}5$ (day) and $Y_0 = 1\text{e-}7$ (night)



(a) Daytime (b) Nighttime

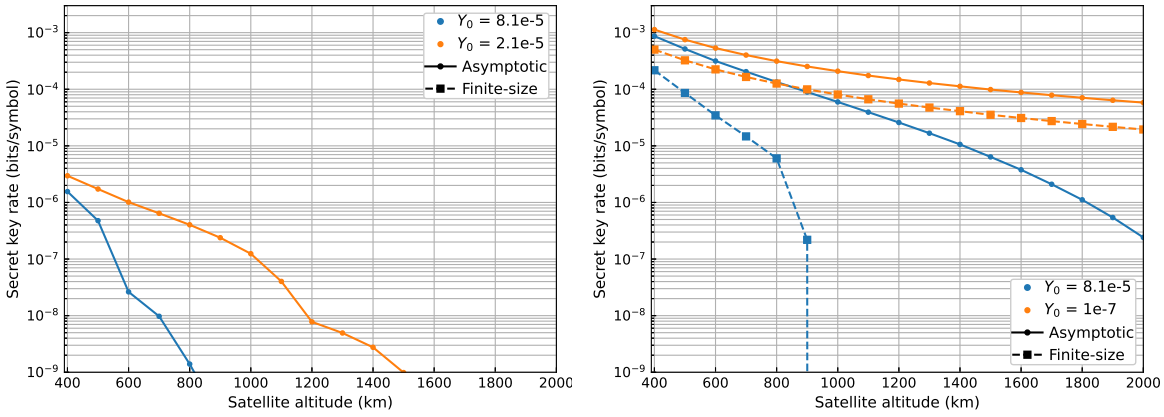
Figure 3.15: Finite-size secret key rate of the CV-QKD protocol for different AO corrections at $h = 500$ km. $\xi_{fix} = 0.03$.

Figures 3.14 and 3.15 show the finite-size key rate results at different turbulence strengths for the DV and CV protocols respectively. This was done for a satellite at 500 km altitude and for mid to low noise levels.

The key rates for the nighttime turbulence conditions are higher than for daytime, which is to be expected since the channel suffers milder turbulence effects and thus has a higher transmission efficiency. This means that under these circumstances, less AO correction is needed. Indeed, we can see a significant increase of the key rate when going from 5 to 10 corrected radial orders but a reduced improvement for corrections beyond that.

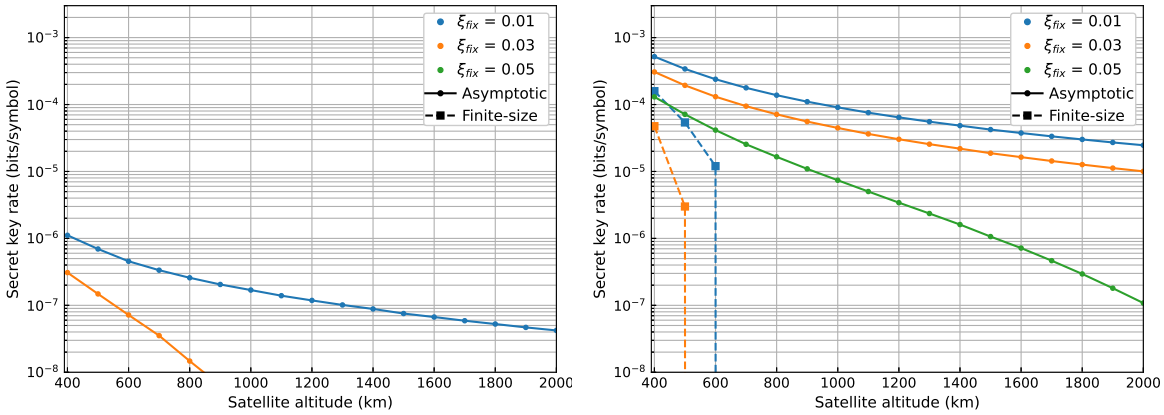
For daytime, since turbulence is stronger and therefore the coupling is more significantly impacted, the introduction of adaptive optics allows for a considerable improvement of the key rate. Instead of the saturation effect observed for nighttime, for daytime conditions the key rate keeps increasing steadily for higher AO correction. This is particularly true for the more severe turbulence profiles where below a certain level of correction it is not at all possible to obtain a key in the finite size regime. An adaptive optics system capable of correcting up to at least 15 radial orders is necessary if we want to obtain a key rate in all turbulence conditions considered in both day and nighttime for both protocols. AO correction beyond that, will increase the key rate for daytime but only have a minimal effect on nighttime at the cost of significantly complexifying the AO system.

We decided to analyze also, how a system without AO correction would perform under our baseline turbulence conditions. Figures 3.16 and 3.17 show the resulting key rate when considering the ground station has no sophisticated adaptive optics and only counts with a fast tip-tilt compensation, i.e. only capable of correcting one radial order ($n_r = 1$), since that is a minimal requirement for most optical ground stations. This was done for altitudes within the Low Earth Orbit range (400 km to 2000 km) and for the baseline D_2 and N_2 turbulence profiles.



(a) Daytime (b) Nighttime

Figure 3.16: Secret key rate of the DV-QKD protocol with only tip-tilt correction.



(a) Daytime (b) Nighttime

Figure 3.17: Secret key rate of the CV-QKD protocol with only tip-tilt correction.

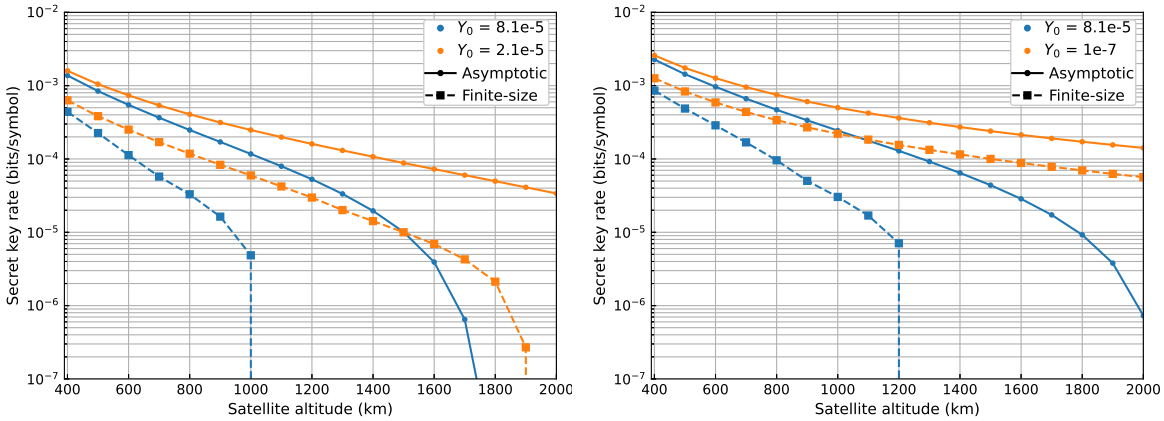
For the DV protocol, we studied the case with the pessimistic background noise level Y_0 = 8.1e-5, as well as more benevolent Y_0 = 2.1e-5 and Y_0 = 1e-7 values for day and night respectively. For the CV protocol in figure 3.19, we considered fixed excess noises of ξ_{fix} = 0.01, 0.03 and 0.05 SNU.

As is to be expected, the performance of both protocols consistently degrades with increased satellite altitude. In the case of the DV protocol, the impact of uncorrected turbulence effects is much more noticeable during daytime where the key rate in the asymptotic regime is greatly impacted. Extraction of a key would be limited only to the lower satellite altitudes. When taking into accounts finite-size effects, it is in fact not possible to obtain a key at all at any altitude for our reference daytime profile. In the case of the CV protocol, the key rate is more severely impacted by the lack of correction. Only satellites at altitudes below 600 km would be able to perform a CV-QKD exchange resulting in any key (accounting for finite-size) during nighttime, and solely for the two systems with the lower excess noises. During daytime, no key can be obtained when considering finite-size effects and the asymptotic key rates are very low, under 10^{-6} bits/symbol.

It is clear that a tip-tilt only correction is not very satisfactory, therefore, since a system correcting up to 15 orders is technologically within reach [88] and a good compromise between complexity and performance, we will consider it as our baseline AO correction in our analysis.

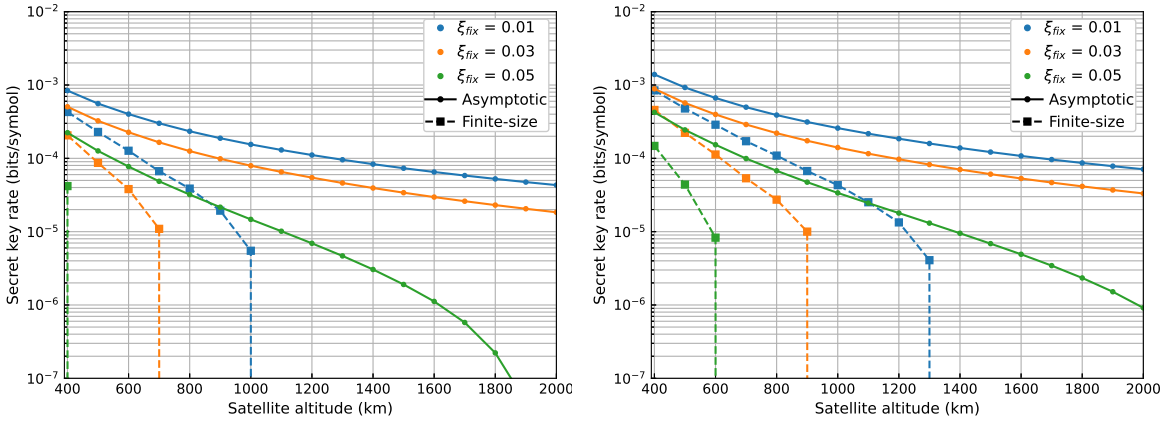
For comparison with the reference tip-tilt case, we now analyze the effect satellite altitude has on the secret key rate performance for our baseline turbulence profiles D_2 and N_2 and considering an AO system correcting up to 15 radial orders. We computed the key rate for the two protocols both in the asymptotic regime and taking into account

finite size effects and the results are illustrated in figures 3.18 and 3.19.



(a) Daytime (b) Nighttime

Figure 3.18: Secret key rate of the DV-QKD protocol versus satellite altitude.



(a) Daytime (b) Nighttime

Figure 3.19: Secret key rate of the CV-QKD protocol versus satellite altitude.

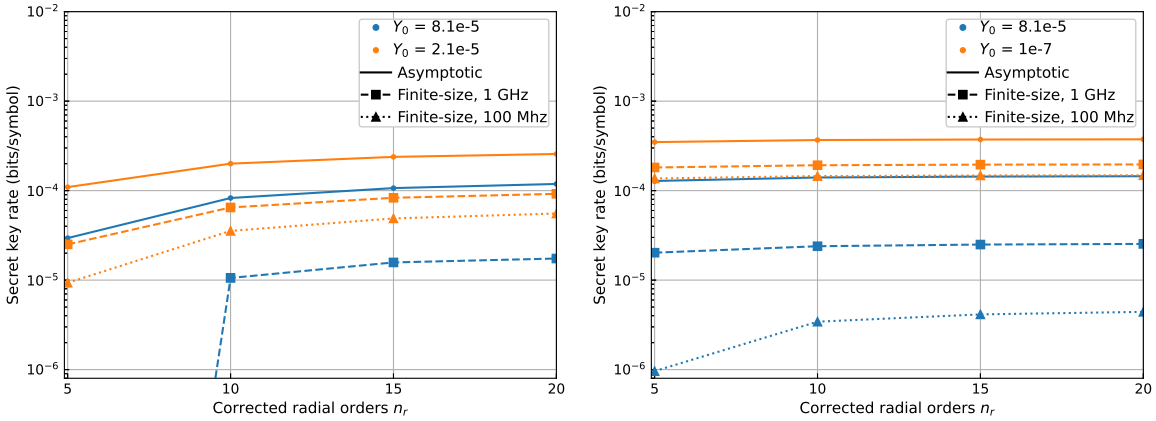
In the case of the DV protocol, at nighttime it is possible to obtain a key for all LEO altitudes in the asymptotic regime, similarly to the case with only tip-tilt correction. However, the performance when taking into account finite-size effects is very clearly improved by the increased correction. For both the low and high noise case, the overall key rates achieved were higher. In addition to that, for the high noise case it is now possible to obtain a key at altitudes of up to 1200 km in comparison with the 900 km altitude reachable with only tip-tilt correction.

Performance at daytime is more significantly improved, the asymptotic key rate is above the tip-tilt 10^{-6} bits/symbol upper limit for all altitudes in the low noise case and for altitudes of up to 1700 km in the high noise case. Most notably, when analyzing the finite-size key rate we observe that higher order correction now allows for the extraction of a key at satellite altitudes of up to 1000 km and 1900 km for the high and low noise cases respectively.

Regarding the CV protocol, the performance is greatly enhanced by the correction of higher orders. For 0.01 and 0.03 excess noise values it is possible to obtain a key in the asymptotic regime for both daytime and nighttime, with the higher 0.05 noise allowing for a key at all altitudes during nighttime but only up to 1800 km during daytime. Finite-size effects however, seem to impact the CV protocol more severely than they did DV. For all ξ_{fix} cases considered, it is only possible to extract a key for low satellite altitudes. In the highest noise scenario ξ_{fix}, it is only possible to obtain a key for satellites at 400 km altitude during daytime. The satellite altitudes reachable during nighttime increase from 800 km to 1300 km, from 500 km to 900 km and from 0 to 600 km for $\xi_{fix} = 0.01$, 0.03, and 0.05 SNU respectively when compared to the tip-tilt only reference case.

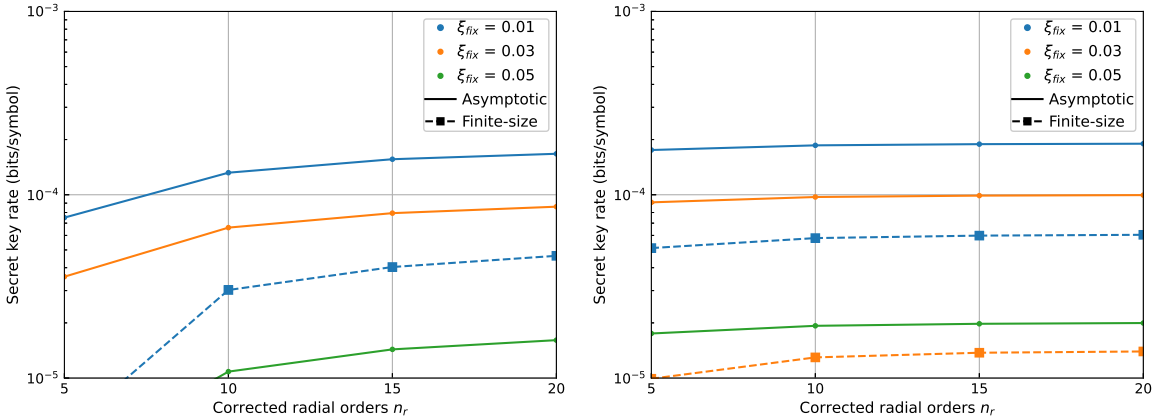
From this comparison we can see that while under some specific circumstances satellite QKD could be still performed with only basic tip-tilt compensation, the use of a higher order AO system has an important role in extending the feasibility of a key exchange and increasing the overall key rate.

As an additional part of our study, we decided to analyze the effect of reducing the size of the receiving aperture at Bob's ground station. Figures 3.20 and 3.21 show the key rate of the DV and CV protocols as a function of the amount of radial orders corrected by the AO system, for a case where the receiver telescope diameter is $D = 80$ cm instead of 1.5 m as was the case in the previous results.



(a) Daytime (b) Nighttime

Figure 3.20: Key rate of the DV-QKD protocol for the 80 cm telescope



(a) Daytime (b) Nighttime

Figure 3.21: Secret key rate of the CV-QKD protocol for the 80cm telescope

In the case of the DV protocol, we show the asymptotic key rate as well as the finite-size key rate for two different source rates, 100 MHz and 1 GHz. This is because, for the pessimistic noise level, a 1 GHz source was required in order to obtain a positive key rate during daytime. For the low noise and daytime scenarios however, 100 Mhz was sufficient to obtain a key. As we can see, apart from a small increase when going from 5 to 10 corrected radial orders, the key rate is not very affected by AO correction, complex AO gives only a small advantage in most configurations.

For the CV protocol, it was not possible to obtain a key in any noise scenario with a 100 MHz source so all the finite-size results displayed correspond to a 1 GHz source.

During nighttime, the AO correction does not seem to have a very significant impact on the key rate. During daytime, performance improves considerable when correcting 10 radial orders, with only a slight increase at 15 and 20 orders. When considering the highest noise value $\xi_{fix} = 0.05$ SNU, the CV protocol would not be feasible at all. The lessened impact of adaptive optics can be explained because the residual phase error increases with the diameter of the receiver. Therefore, systems with smaller telescope diameters are less affected by turbulence. However, the light captured by a smaller telescope is lower, increasing the overall losses of the channel. It is thus possible to establish a satellite-to-ground link with a smaller receiving telescope without the assistance of adaptive optics, but only for very specific circumstances of nighttime operation like low noise and a high rate source.

3.5 Conclusion

The results of the simulation process detailed in this study show that there is a strong interest to the use of adaptive optics in satellite-to-ground links in order to improve the secret key rate performance of both discrete variable and continuous variable QKD protocols. This is particularly noticeable for daytime turbulence conditions, in which a complex AO correction is necessary for operation, and for the CV-QKD protocol which is more susceptible to losses and thus can greatly benefit by the increased transmission efficiency of a system correcting higher orders.

Expanding on these results can be done in several ways but we will focus on the two we have found to be the most straightforward: extending the analysis to a multi-link case where the transmission efficiency of different channels is simultaneously taken into account, and providing an experimental validation of the simulation model we have employed. We will present the simulation results corresponding to the multi-link approach in chapter 4 and in chapter 5 we will detail the advances we have made towards the experimental validation approach.

Chapter 4

Multi-link satellite-to-ground QKD with adaptive optics

In the previous section we could observe that a simple QKD link between a satellite and a ground station could be feasible in certain circumstances, and significantly improved by the use of adaptive optics. We now would like to test the effectiveness of AO correction and model the behavior of a multi-link QKD scenario. In the following, we will give a brief overview of the state of the art, a description of the scenario considered and a description and analysis of the simulation process and the final estimated performance of such a system.

4.1 State of the art

The implementation of multi-link QKD is a research topic of particular interest in the context of the creation of a large scale quantum communications network. While the type of links explained in the previous section, allows for a satellite to share a key with a ground station making their communications secure, a more common necessity would be to establish a shared key between two ground stations. If the ground stations are located at great distance from one another, one promising option would be to employ a satellite as an untrusted node in order to distribute the secret key to the stations.

Such is the idea behind the utilization of entanglement based QKD (EB-QKD) satellite links where the satellite generates a pair of entangled photons, with each photon being sent to a different ground station. This kind of architectures, like the BBM92 protocol we aim to study, are a very promising alternative in order to reach inter-continental communication distances. Several theoretical studies have been performed in order to assess the viability of satellite-based, or more generally, free-space EB-QKD. Some of the aspects considered include the employment of non-maximally entangled states with the BBM92 protocol [89] as well as the effect of high losses on the Quantum Bit Error Rate (QBER) of entanglement-based protocols [90]. Some theoretical studies have also analyzed the potential improvement of the link efficiency for quantum protocols when

employing adaptive optics, but in an uplink scenario [91] or focusing on non-EB protocols.

Multiple experimental works have also been published, focusing on the design of QKD sources for satellite QKD [92], the implementation of entangled protocols over considerable free-space distances [93] (15 km) and even the operation of free-space EB-QKD in daylight over short distances [94, 95] among other things. Regarding the inclusion of adaptive optics, some experiments have been done but often focusing on protocols other than the BBM92 like some analyzing the effect of AO entanglement conservation for orbital-angular-momentum entanglement [96], or the impact on key rate for an entanglement version of the BB84 protocol [97].

Probably the most notable experimental implementation however, was once again performed with the equipment aboard the Micius satellite [31]. One of the multiple quantum experiments performed by this satellite was the execution of an entanglement based key exchange between two Chinese cities 1200 km apart. The exchange was performed at nighttime, had a duration of around 3000 seconds and resulted in an estimated asymptotic key rate of 0.43 bits/s, a finite-size key rate of 0.12 bits/s and an estimated QBER of around 4%. This exchange was performed with free-space single photon detectors, so no single-mode fiber coupling was involved.

With most current literature focusing on nighttime operation, short free-space distances or otherwise not including AO correction, we would like to focus on studying the performance of the BBM92 protocol in daytime assisted by adaptive optics.

4.2 Scenario

The scenario we have chosen to consider for this study is illustrated in figure 4.1. We will analyze the implementation of a BBM92 protocol where a LEO satellite (Charlie) can generate entangled photon pairs at telecom wavelength. Each photon from the pair is then sent to one of two optical ground stations (OGS), Alice's or Bob's. Both ground stations will be equipped with adaptive optics correction systems, whose influence on the performance we aim to examine. Since the satellite has to be able to communicate with both ground stations at the same time in order to perform a key exchange, we will only consider the segment of the satellite's trajectory in which both Alice and Bob can observe it at more than 20° of elevation.

Similarly to the single-link case, we assume Charlie emits a beam with a certain divergence θ_d and pointing error θ_p. For the sake of simplicity, Alice and Bob's ground stations are nearly identical, both have receiving apertures of diameter D placed at height h_T and both couple the received light into an optical fiber after applying an adaptive optics scheme capable of correcting up to n_r radial orders. We consider as

well the same turbulence profile for both ground stations, the reference daytime profile from our previous study, D_2. However, we account for the elevations of each OGS, and we generate independent turbulent channel occurrences.

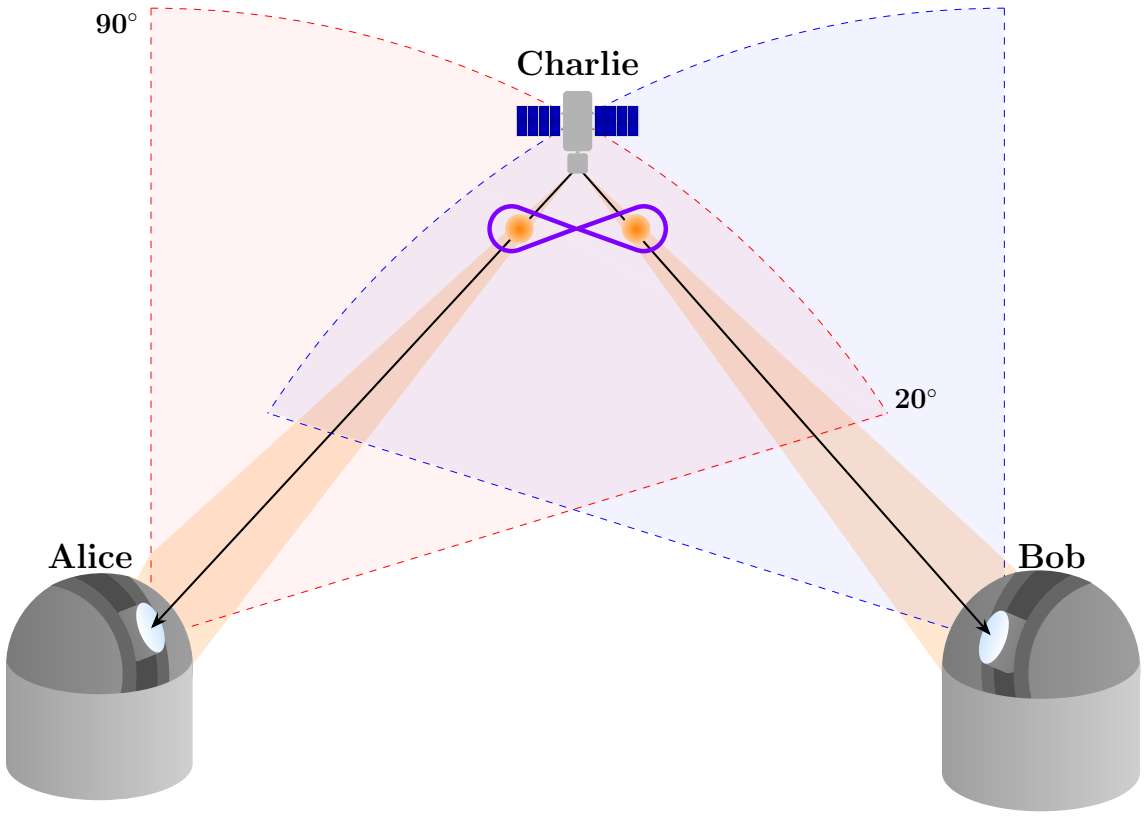


Figure 4.1: Entanglement-based quantum key distribution scenario between a LEO satellite and two ground stations.

We assume Charlie is following the same orbit as the Micius satellite for a given satellite pass, and we consider that it is capable of generating entangled photon pairs at a rate μ. In the context of a future European quantum network, we will consider two key distribution scenarios, one where Alice and Bob are located in Paris and Nice, and another where they are located in Nice and Matera.

4.2.1 Reference values

In the following, we will detail the reference values of the main parameters involved in this study, many of which were specifically chosen based on the single-link analysis from the previous section, in particular the ones employed for the analysis of the discrete variable protocol BB84.

Parameter	Symbol	Value
Wavelength	λ	1550 nm
Pointing error	θ_p	1 μrad
Divergence	θ_d	10 μrad
Zenith transmittance	τ_{zen}	0.91
Pair generation rate	μ	$11.4{\cdot}10^6$ pairs/s
Receiver diameter	D	1.5 m
Receiver altitude	h_T	5 m
AO loop frequency	f_{AO}	5 kHz
AO loop frame delay	δ_t	2 frames
Wavefront projection	n_{rmax}	40 radial orders
Fiber/receiver ratio	D/w_z	2.2
Detection efficiency	η_d	0.85
Dark counts	$d_{a(b)}$	$4.2{\cdot}10^4$ counts/s
Zenith Fried parameter	r_0	10.6 cm
Zenith isoplanatic angle	θ_0	25.8 μrad
Temporal window	Δt	500 ps
Correctness parameter	ε_{corr}	10^{-10}
Security parameter	ε_{sec}	10^{-10}
Error correction efficiency	f_{EC}	1.16

Table 4.1: General simulation parameters for the entangled photon protocol

The detection efficiency corresponds once again to highly efficient SNSPDs whose utilization is made possible by coupling the received light into a fiber. The effect of the AO correction will be examined by considering systems capable of correcting up to $n_r = 1$, 5, 10, 15, or 20 radial orders. The pair generation rate $\mu = 11.4{\cdot}10^6$ pairs/s corresponds to the state-of-the-art for telecom wavelength entangled photon sources [98]. We consider as a baseline, the same level of daytime background noise as the less pessimistic case assumed for the BB84 protocol, that is $Y_0 = 2.1{\cdot}10^{-5}$, which corresponds to a dark count rate of $d_{a(b)} = 4.2{\cdot}10^4$ counts/s. The Micius satellite, follows a sun-synchronous elliptical orbit with perigee and apogee altitudes equal to 488 km and 584 km respectively.

4.3 Simulation

The simulation process is very similar to the one illustrated in figure3.2. This time however, we have to take into account the behavior of two atmospheric channels, one between Charlie and Alice and the other between Charlie and Bob. For each point in the trajectory of the satellite, we simulate (independently) the coupling efficiency statistics and the transmission statistics due to beam wandering (stages 2 and 3 of our previous process) for both channels. Then, we combine them as before, resulting in

the transmission efficiency statistics $\mathbf{PDTE}_{\varepsilon}$ for each channel, which correspond to the specific elevations ε_A and ε_B. This allows us to estimate the coincidence rate R_c at each instant of the trajectory, as well as the bit error rate which will ultimately allow us to estimate the secret key rate of the protocol.

In order to simulate the performance of the exchange, we first need to estimate the trajectory of the satellite in regard to the ground stations. To estimate the channel efficiency at any given point of the satellite pass, it is necessary to know the distance to the satellite and the elevation at which the ground station can observe it. The way this was estimated, was through the two-line element set (TLE) coordinates of the Micius satellite. TLE is a data format encapsulating orbital information of a satellite for a given point in time. With the knowledge of the TLE information of a satellite and with an appropriate prediction algorithm, it is possible to determine the position and velocity of the satellite at any given moment. The prediction algorithm we employed, is part of the open-source space dynamics library *Orekit* [99].

As mentioned before, we will be considering two scenarios, *scenario 1* is an exchange between the satellite, a ground station in Paris and the other in Nice and *scenario 2*, corresponds to a key exchange involving a ground station in Nice and another one in Matera, Italy. Given the satellite's TLE and each of the ground station's GPS coordinates, the orekit propagator allowed us to estimate the distance and elevation at which the ground stations observe the satellite for a given satellite pass. We chose two passes of the satellite, both in 2023, one for each scenario considered. The resulting distances and elevations estimated can be observed in figures 4.2 and 4.3.

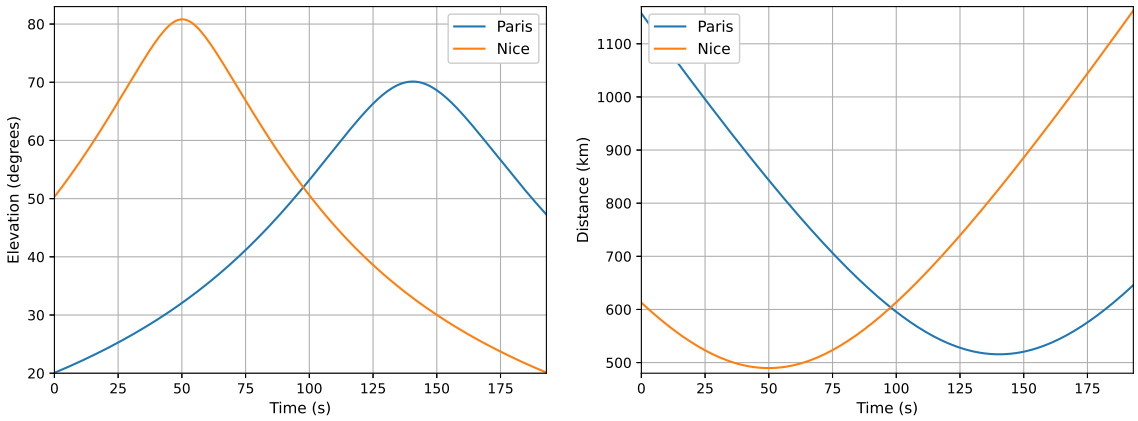


Figure 4.2: Elevation and distance to the Micius satellite from the Paris and Nice ground stations. Scenario 1.

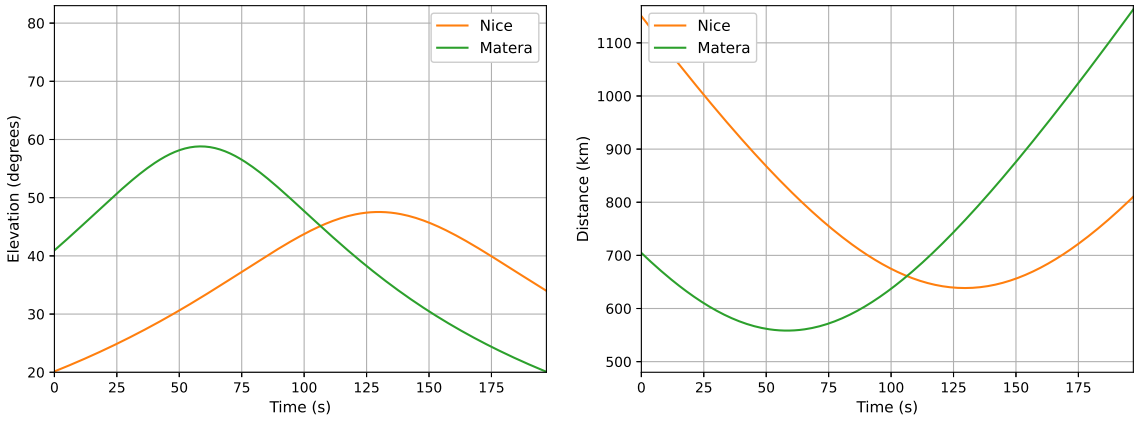


Figure 4.3: Elevation and distance to the Micius satellite from the Nice and Matera ground stations. Scenario 2.

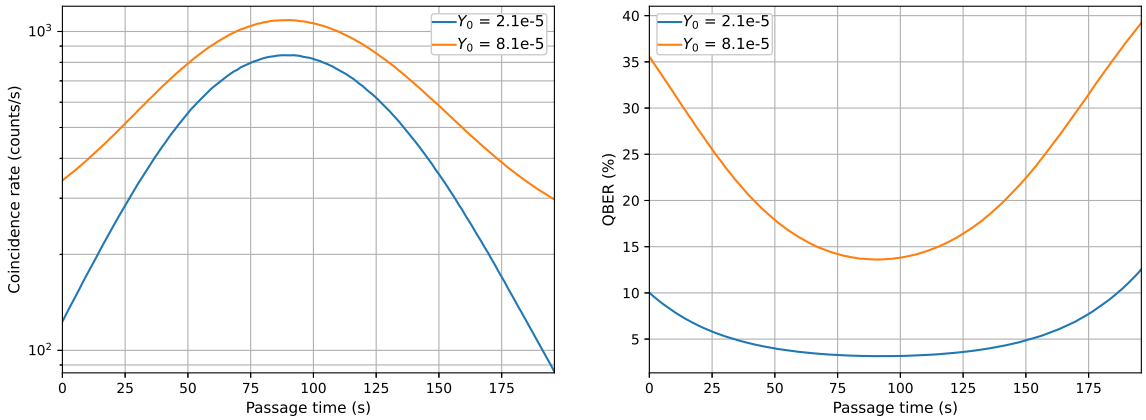
As we can see, in both scenarios, the distances from each ground station to the satellite are significantly different from one another. It should be noted that in the Paris-Nice scenario, it is possible to observe the satellite at considerably higher elevations than in the Nice-Matera scenario, resulting in generally lower losses. This is partially due to the fact that Nice and Matera are located further away from each other and partially due to the dynamics of the satellite orbit.

Each scenario will thus involve two different atmospheric channels. In *scenario 1*, channel A corresponds to the atmospheric channel between the satellite and the Paris ground station while channel B is the one between the satellite and the Nice ground station. Similarly, for *scenario 2*, channel A is the satellite-Nice channel and channel B is the satellite-Matera link. Since we are considering different satellite passes for each scenario, it is important to note that while channel B from scenario 1 and channel A from scenario 2 both involve the Nice ground station, the loss suffered by the channels will be different as evidenced by the differing elevations and distances shown in figures 4.2 and 4.3.

With the trajectories of the satellite having been calculated, we decided to divide them in 150 temporal intervals in order to estimate the transmission efficiency of the channels at each point in time. Each interval corresponds to a specific elevation ε_A and distance R_A for channel A and a different elevation ε_B and distance R_B for channel B. For every interval, we compute the coupling efficiency statistics P_{AO} and the transmission efficiency statistics P_{BW} for both channels and combine them into the total probability distributions $PDTE_{\varepsilon_A}$ and $PDTE_{\varepsilon_B}$ through the same process as described in equation 3.3.2. This gives us a probabilistic description of $\tau_A = \mathrm{T}_A^2$ and $\tau_B = \mathrm{T}_B^2$ at every point of the trajectory.

Based on this, we are able to estimate the expected value of the coincidence rate R_c and the bit error rate ϵ via equations 1.2.8 and 1.2.11 respectively.

We first wanted to examine the effect of background noise on the key exchange. We chose scenario 2 (Nice-Matera) as an example, considering turbulence profile D_2 and an adaptive optics system capable of correcting up to 15 radial orders, the standard correction level we settled upon for our previous study. We estimated the mean coincidence rate and QBER for two different noise levels, $Y_0 = 8.1{\cdot}10^{-5}$ and $Y_0 = 2.1{\cdot}10^{-5}$, the same noise cases considered for the BB84 protocol. These 0-photon yields are considered equal for both ground stations and correspond to total dark count rates of $d_{a(b)} = 16.2{\cdot}10^4$ counts/s and $d_{a(b)} = 4.2{\cdot}10^4$ counts/s respectively. Figure 4.4 illustrates the results we obtained.



(a) Coincidences

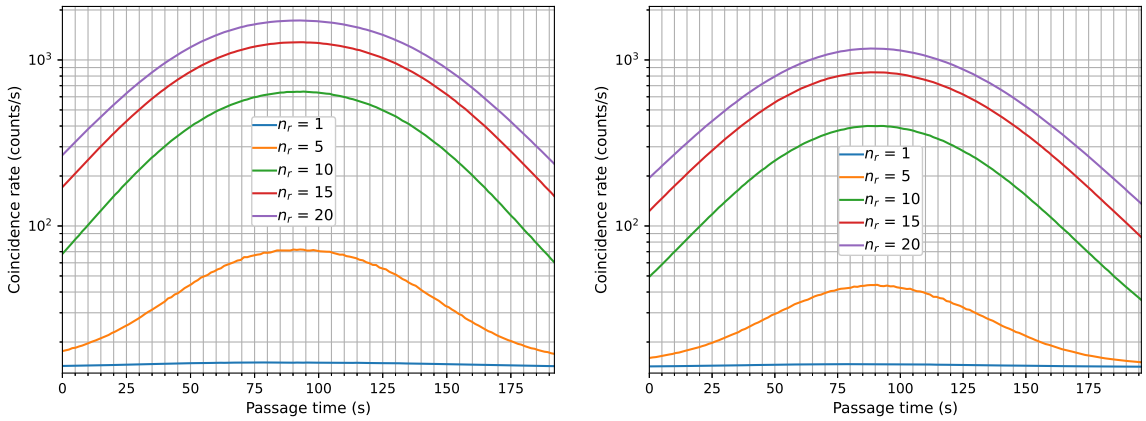
(b) QBER

Figure 4.4: Coincidence rate and QBER for low and high background noise levels.

We can observe that the coincidence rate for the high noise scenario is more elevated than the one for the low-noise case. While this may seem counterintuitive at first, we have to take into consideration the fact that part of the coincidences measured occur when no photon pair was emitted and are thus errors. Having a higher background noise will result in more erroneous detections and therefore in an increased R_c. This can be further evidenced in the resulting QBER graph, where the error rate for the high-noise pessimistic case is found to be considerably higher, reaching up to almost 40% error in comparison to the low-noise case whose error remains below a 15% threshold for the entire pass. The error is such that no positive key rate could be estimated for the pessimistic scenario, because of this, further analysis is performed only in the $Y_0 = 2.1{\cdot}10^{-5}$ noise case.

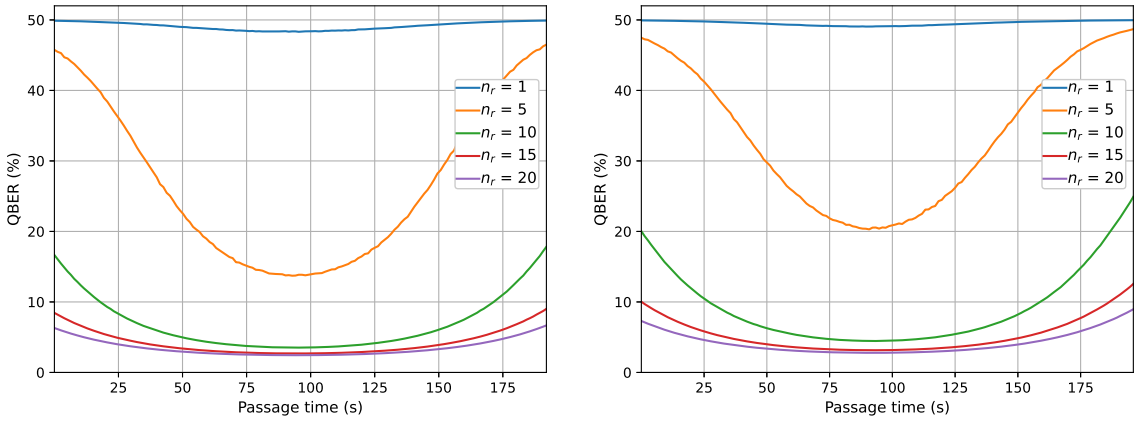
The main parameter we intend to examine is how the adaptive optics correction

affects the performance of this entanglement based protocol. We therefore simulated the coincidence rate and bit error rate for both of the scenarios considered for AO systems correcting $n_r = 1$, 5, 10, 15 and 20 radial orders. For simplicity, we consider both Alice's and Bob's ground stations have the same correcting capabilities and the turbulence profile considered for the coupling efficiency simulations of both channels the D_2 daytime profile. The coincidence rate and QBER results can be found in figures 4.5 and 4.6 respectively.



(a) Paris-Nice (b) Nice-Matera

Figure 4.5: Coincident count rate for different number of corrected orders



(a) Paris-Nice (b) Nice-Matera

Figure 4.6: Quantum bit error rate for different number of corrected orders

We observe that the coincidence rate for the Paris-Nice scenario is slightly higher than the one for the Nice-Matera case and the error rate is moderatly higher. This is

consistent with the trajectory estimated since in the second scenario the ground stations are farther away from the satellite and therefore losses are higher. In both scenarios, when there is no specialized AO correction $n_r = 1$, the rate at which photons are detected by both stations is extremely low. Employing a system capable of correcting as little as 5 radial orders already results in a significant increase of R_c, with an even more important improvement when going to up to 10 corrected orders. Further AO correction keeps augmenting the coincidence rate but the difference of performance between correcting 15 and 20 radial orders is not as meaningful.

Regarding the behavior of the QBER, when there is no adaptive optics beyond tip-tilt correction the error rate is exceptionally high, about half of all coincidental detections are erroneous. While correcting up to 5 radial orders decreases the QBER significantly, at least 10 order correction is necessary in order to have less than 20% error, still a quite high error margin. In order to ensure an error below 10-15%, it is necessary to consider an AO system capable of correcting 15 or 20 radial orders.

4.4 Key rate estimation results

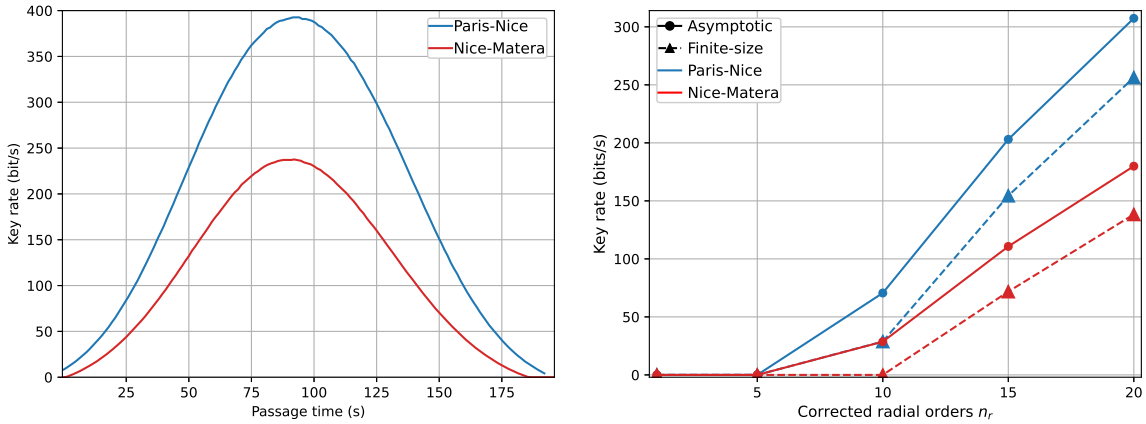
Having computed the intermediary performance metrics of coincident count rate R_c and QBER ϵ, it is now possible to estimate the key rate of the protocol both in the asymptotic regime and taking into account the finite-size effects. Through equation 1.2.7 it is possible to obtain the instantaneous asymptotic key rate throughout the satellite pass. Figure 4.7a illustrates this for both the Paris-Nice and Nice-Matera scenarios when considering an AO correcting up to 15 radial orders.

The difference of performance of both scenarios is slightly more evident here. The Paris-satellite-Nice links have fewer path losses and better coupling into the fiber as a result of smaller distances to the satellite and higher elevation. The effects of this can be already observed on the lower coincidence rate and higher error rate, but it is clearer when looking at the instantaneous key rate. In the Paris-Nice scenario, it is possible at the best point in the satellite pass to obtain an asymptotic key rate of almost 400 bits/s. In contrast, the values reached for the Nice-Matera link are considerably lower, never surpassing 240 bits/s.

In order to provide a more realistic assessment of the situation however, we also computed the BBM92 key rate taking into account finite-size effects as per equation 1.2.13. The importance of this analysis is significantly more concrete when observing the very limited time in which the satellite can communicate with both ground stations, not significantly longer than 3 minutes, between 190 and 200 seconds. We assume that the key rate is extracted from the entire block of information exchanged during those 200 seconds and thus the total coincidental counts C_T are the sum of all counts depicted

in the previous section.

Figure 4.7b depicts the average key rate for an entire satellite pass for both scenarios in the asymptotic regime and including finite-size effects. As we can see it is not possible to extract a key in the atmospheric conditions considered, without adaptive correction or when correcting very few radial orders. For the more optimistic Paris-Nice scenario, correction of up to 10 radial orders already makes it possible to obtain a key even under finite-size constraints. However, in order to ensure the performance of the system even under less idealistic circumstances such as the ones from the Nice-Matera scenario, it is necessary to consider a more sophisticated correction scheme, capable of compensating for at least 15 radial orders.



(a) Asymptotic key rate

(b) Average key rate vs corrected orders

Figure 4.7: Key rate estimation for the Paris-Nice and Nice-Matera scenarios.

4.5 Conclusion

In this simulation study we are able to show that the implementation of a BBM92 protocol could be feasible during daytime when aided by an adaptive optics correction system in order to improve signal coupling into a fiber. Increasing the correction capacity and thus the complexity of the AO system results in improved key rates. With a moderately complex system that is still within technological reach, capable of correcting up to 15 radial orders, it is possible to obtain average key rates of up to 150 bits/s, meaning approximately 30 kbits of key could potentially be exchanged during a satellite pass.

Chapter 5

Towards an experimental demonstration

In the previous sections we have explained our detailed modelling of atmospheric effects and their impact on the performance of various QKD protocols. It was shown that the use of an adaptive optics correction system can significantly improve the secret key rate by increasing the coupling into a single mode fiber. The next logical step in order to verify the validity of these simulation results is an experimental proof-of-principle demonstration in a laboratory environment. In the following, we will explain the advances we have made towards this goal and the different considerations we have to take into account for its execution.

5.1 CV-QKD with atmospheric channel

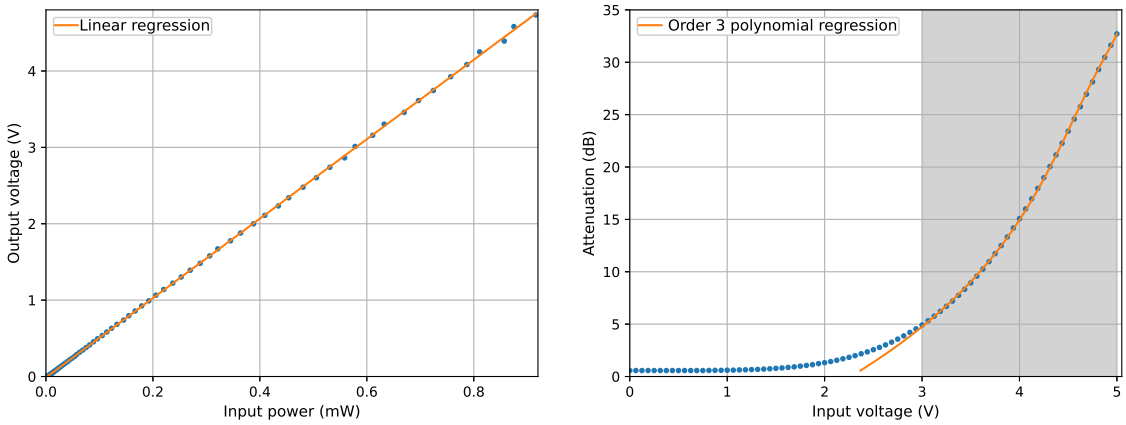
While the most direct way of assessing our models would be to test the effect of AO on a LEO-to-ground quantum exchange, it is evidently not easy to implement. Therefore, in the absence for the moment of access to a satellite with a quantum payload and a ground station equipped with an adaptive optics system, we can emulate the conditions of the satellite channel within the laboratory in a simpler implementation as a first validation step which can be helpful for designing future missions.

A first approach is to employ an already existing QKD experimental setup, and reproduce the effects of the atmospheric channel between Alice and Bob, in order to see how such a system would bear the impact of high attenuation that varies in time. We will first show how we intend to emulate the atmospheric channel, and then we will explain how the existing CV-QKD experimental bench at LIP6 works and the challenges we encountered when attempting to use it in conjunction with the channel.

5.1.1 Atmospheric channel emulation

A simple simulation of the attenuation on the channel due to atmospheric effects could be achieved by employing an electronic variable optical attenuator (VOA). We have chosen to use the Thorlabs *V1550PA* [100], a VOA that applies a certain attenuation to the input optical signal, depending on the driving voltage. This device is based on MEMS technology, it uses a polarization maintaining fiber, it has a range of attenuation between 0 and 30 dB, and its electrical input can be modulated up to a frequency of 1 kHz.

The first step in order to correctly represent the satellite-to-ground channel is thus to characterize the VOA in order to accurately determine how the attenuation varies as a function of the applied voltage. This was done via a simple optical setup with a 1550 nm continuous wave laser connected to the optical input of the VOA and a photodiode connected to the output. With the help of a National Instruments data acquisition system (USB 6363), we varied the input voltage of the VOA while recording the output voltage of the photodiode. It was therefore necessary to characterize the photodiode (*PDA05CF2*) as well, to know the relation between the voltage returned by the NI card and the actual optical power received. This characterization can be found in figure 5.1a and the relation between input power P_{in} and output voltage V_{out} can be very well approximated through a linear regression as such: $V_{out} = 5200.53 \cdot P_{in} - 0.013$.



(a) Photodiode (b) VOA

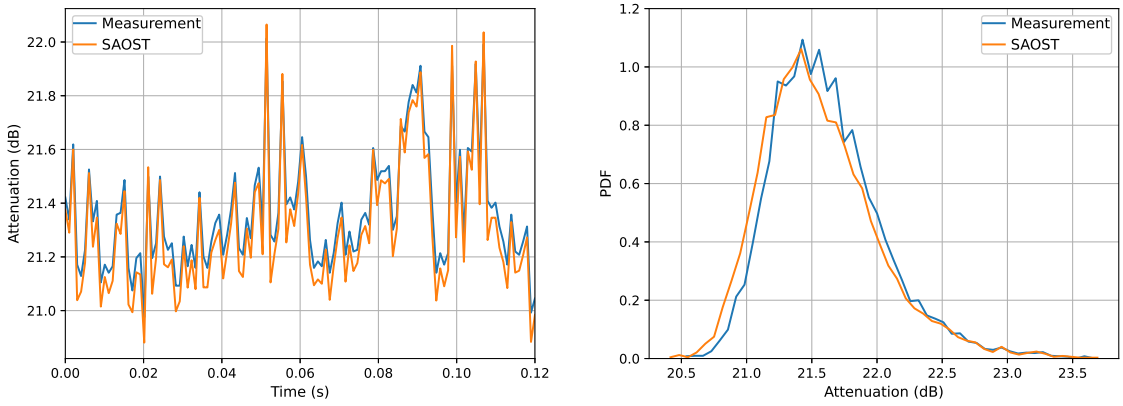
Figure 5.1: Characterization of the components for the channel emulator

With the knowledge of the optical power detected, it is then possible to determine the attenuation applied at a specific voltage by subtracting from the original power (in dBm) at the laser output. The VOA characterization results can be observed in figure 5.1b. The first thing to notice is that even with a 0 V input, using the VOA results in some attenuation due to the insertion losses which amount to approximately 0.57 dB.

For low input voltages, the change in attenuation is minimal, so we focus on the section between 3 and 5 V (highlighted in the figure), in which small variations in the voltage have a much more significant impact on the attenuation applied, giving us a working range of attenuation between 5 and 32 dB. In this range, it is possible to approximate the behavior of the VOA by a third order polynomial, with the input voltage V_{VOA} necessary to apply attenuation Att (in dB):

$$V_{VOA} = 6.9 \cdot 10^{-5} Att^3 - 5.08 \cdot 10^{-3} Att^2 + 0.18 \cdot Att + 2.27 \tag{5.1.1}$$

With the help of the modified SAOST simulation tool that takes into account path loss and beam wandering, it is possible to generate a time series of the attenuation suffered by the channel under certain atmospheric conditions. In order to test how accurately we can replicate the attenuation of the channel, we generate a time series, estimate the input voltage we need to apply and measure the resulting attenuation with the help of the photodiode. Figure 5.2 shows the results of this comparison for a link at 30° elevation, a satellite altitude of 400 km, D_2 turbulence profile and an AO capable of correcting up to 15 radial orders. The series of voltages corresponding to the SAOST time series was applied at 1 kHz, the maximal modulation speed of the VOA.



(a) Time series

(b) Probability distributions

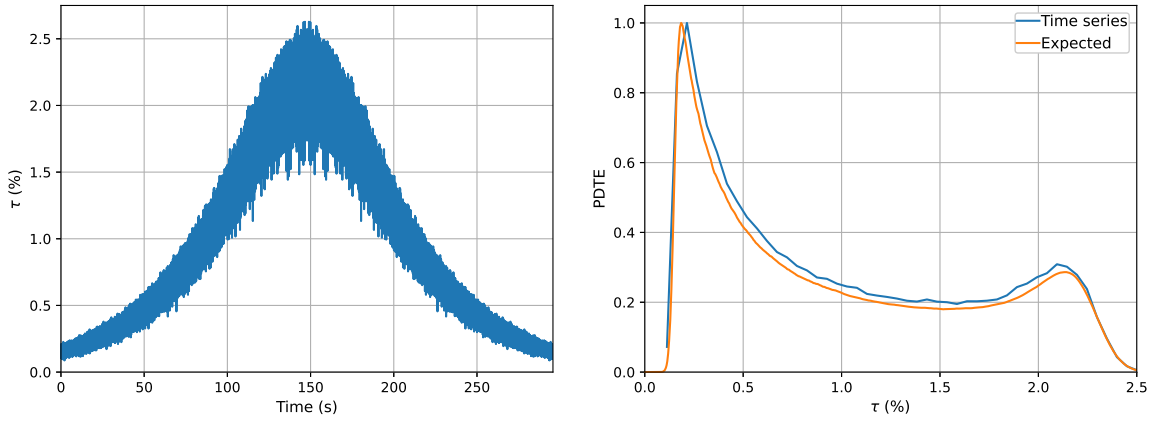
Figure 5.2: Comparison between SAOST generated time series and the attenuation measured and their corresponding probability distributions.

As we can see, the attenuation that was actually measured closely follows the intended attenuation estimated through the simulation tool. When comparing the expected and measured attenuation values of various time series for different elevations, we found that the average error was between 0.03 and 0.14 dB. In figure 5.2b, we can observe the probability distribution of the attenuation for a SAOST time series consisting of 10000 occurrences as well as the probability distribution of the actual attenuation measured when applying the series over 10 seconds. The distributions are very similar,

showing that the VOA can accurately replicate the attenuation variations of the atmospheric channel.

It is important to note that, for very low AO correction, low elevation and high altitude satellites it is possible to exceed the maximal 32 dB attenuation applicable with the VOA. In this case however, it would be possible to add either a fixed attenuator or a manual VOA in order to shift the operating point of the emulating system and thus be able to reproduce very low attenuation values.

With the modified SAOST we can only represent the attenuation at one particular elevation, and we would like to emulate the variation of attenuation with time throughout an entire satellite pass. In order to do that, we estimated the trajectory of the satellite assuming it follows a circular orbit. We consider only elevations above 20°, and we divide the trajectory into 300 sections. The sections have equal duration and correspond to a specific elevation, so we generate a time series of attenuation for each one, and we concatenate all of them into a single time series for the entire pass. An example of such a time series for a D_2 turbulence profile, 15 order AO correction and 500 km altitude can be observed in figure 5.3a and its probability distribution can be found in figure 5.3b.



(a) Time series

(b) Probability distribution

Figure 5.3: Time series and probability distribution of an entire satellite pass for a 500 km satellite, D_2 profile and 15 corrected radial orders.

We compute the probability distribution of the transmission efficiency (PDTE) represented by our concatenated attenuation time series and compare it with the expected PDTE estimated from the simulations in section 3.3.4. As we can see, the distribution of the time series matches quite closely the expected PDTE. This shows that the time series could adequately represent the general behavior of the attenuation (or conversely the transmission efficiency) of the atmospheric channel when applied through the VOA.

5.1.2 CV-QKD experimental setup

The experimental CV-QKD bench present at LIP6 is depicted in figure 5.4 [101].

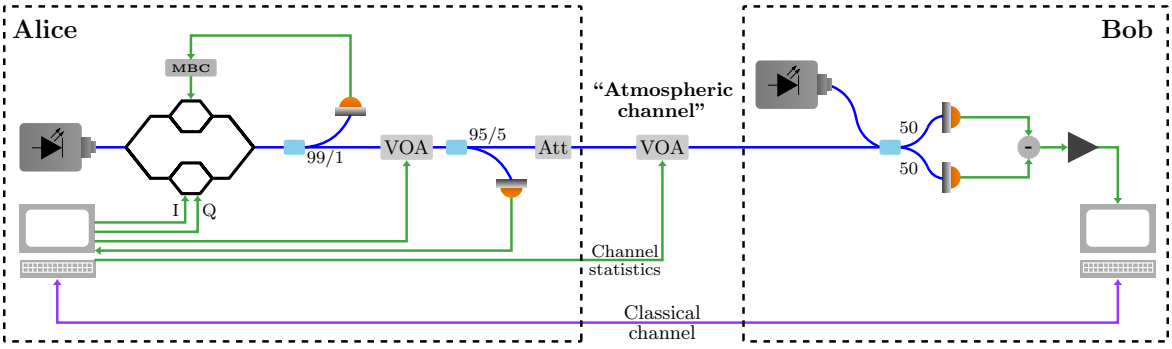


Figure 5.4: Experimental setup of a CV-QKD demonstration

We can observe the three main parts of the experimental setup: Alice, Bob, and in between them our emulation of the atmospheric channel via the electronic VOA. Blue connections correspond to optical links and green connections are electrical links.

Alice's setup consists of a continuous wave laser at telecom wavelength whose optical output is sent to a Mach-Zehder IQ modulator. This device employs the electro-optic effect to modulate the quadratures of the laser pulse by applying an electrical field to the optical signal. Alice has a computer that generates random values of the two quadratures to be sent into the IQ modulator while shaping the continuous signal from the laser into pulses via a root-raised cosine filter. This type of filter is commonly used in classical communications as it reduces the interference between pulses. A 99/1 beam splitter redirects the majority of the optical power into a detector whose signal is utilized by a Modulator Bias Controller (MBC) that injects a dither signal at low frequency and uses it for the feedback loop controlling the bias voltage in order to provide the IQ modulator with the appropriate bias tensions. The rest of the optical signal goes into a VOA and then into a 95/5 beam splitter, most of the signal is detected and used to estimate V_A. The attenuation applied by Alice's VOA, the power of the laser and the variance chosen by software, determines the average number of photons in each coherent state $\langle n_{ph} \rangle$ which dictates the variance of Alice's states as $V_A = 2\langle n_{ph} \rangle$. Knowing the optical power on the photodiode, we can thus estimate the average number of photons at Alice's output.

Finally, a fixed attenuator is added in order to further reduce the amplitude of the optical signal. It is important to note that in addition to the quantum states, Alice sends some classical signals as well to help Bob with signal processing. She sends two frequency-multiplexed *pilot tones* with the quantum signal; these are necessary for clock recovery, frequency recovery and the correction of the relative phase. In order to mark the start of the quantum data, Alice sends a Zadoff-Chu sequence [102]. This sequence

has the particularity of being uncorrelated with any shifted version of itself which aides in the synchronization process to establish the exact beginning of the quantum exchange.

Bob's experimental setup is simpler than Alice's, but its digital signal processing (DSP) functions are more complex. Bob receives the transmitted optical signal after it has been propagated through the channel, and he performs a so-called RF heterodyne detection. In order to implement this type of coherent detection Alice shifts the spectrum of the signal, effectively performing optical single side-band modulation (OSSB), to avoid low-frequency noise. This makes it possible to employ a single beam splitter to mix the received signal with a local local oscillator: upon mixing, the signal is further shifted in frequency by the difference in frequency between the two lasers and the two outputs are received by a balanced detector. The balanced detector then performs the subtraction of the two photocurents and this residual current is then amplified by a trans-impedance amplifier that is acquired by Bob's ADC. By performing frequency demodulation, information on both quadratures is now available to Bob who can thus proceed to apply its DSP functions in charge of filtering, synchronizing and correcting the phase of the signal and will ultimately obtain a series of received quantum symbols [101]. Alice and Bob can then proceed to the parameter estimation stage in which they will determine the transmission efficiency of the channel T^2 as well as the excess noise during the exchange ξ. Knowledge of these parameters allows for the computation of the secret key rate as explained in section 1.3.

5.1.3 Difficulties and perspectives

The CV-QKD system that we adapted for the demonstration has been shown to function correctly at channel attenuations of around 5 dB, the equivalent of propagating Alice's signal through 25 km of single mode fiber. However, the lowest attenuation we would like to emulate with our channel would be of the order of 13 to 15 dB for the lowest altitude satellite and mild turbulence conditions. A direct incorporation of the VOA channel emulator is not possible as several challenges have to be handled.

The first challenge is the covariance between Alice and Bob's symbols, a key element in the parameter estimation process [35]. The covariance found in this setup is too low, hence new DSP algorithms on Bob's side need to be developed in order to better perform phase correction in high attenuation conditions. The quantum signal is low in comparison to the dither noise of the MBC, so a better averaging of the optical power measurement is probably also necessary. With very large values of Alice's variance and a fixed 30 dB of attenuation, it was possible to execute most of the DSP to the point where the parameter estimation stage gave as a result a measured transmission efficiency value T^2 fairly close to the attenuation actually being applied. However, the V_A values that were necessary for this, make it so that the amount of photons per pulse

of normal operation is greatly exceeded.

The next issue to be approached is the fixed excess noise of the setup. In the absence of an eavesdropper, during the characterization of the system, this noise is intrinsic to the specific experimental setup. In this case, the excess noise is measured at Bob's side and was consistently found to be around 0.01 SNU. Within the model that we used for CV-QKD in the atmospheric channel, we assumed an excess noise that is fixed at Alice's side ξ_{fix}, that when measured by Bob could be expressed as $\xi_B = \eta_d T \xi_{fix}$. This means that for a 13 dB attenuation and considering the detector efficiency η_d of the system is approximately 0.45, the excess noise is around $\xi_{fix} = 0.1$ SNU. Figure 5.5 shows the calculated asymptotic key rate as a function of ξ_{fix} for one satellite pass in the different daytime turbulence conditions, at the lowest considered satellite altitude (400 km). As we can see, it is impossible to extract a key even in the optimistic asymptotic regime for an excess noise above 0.087 SNU, which is the main reason why it is not possible to estimate a key rate for the experiment as it is.

Methods of reducing the excess noise of the experimental setup have to be further researched and will probably involve some fine-tuning of the DSP algorithms for high attenuation circumstances. Increasing the number of symbols per frame can improve the accuracy of the estimations based on the covariance matrix. Changes in hardware and the adjustment of other parameters such as improved phase recovery algorithms can also help reduce ξ. Replacing Alice's laser for one with a narrower linewidth, or shifting the signal's frequency away from the IQ modulator's noise can be some alternatives for example.

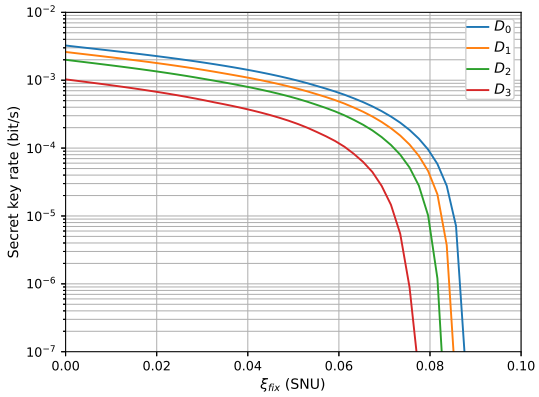


Figure 5.5: Secret key rate vs ξ_{fix} for different daytime turbulence profiles

One last thing to be taken into account is the time it takes to run the experiment. Currently the CV-QKD is capable of performing an exchange between Alice and Bob that lasts around 70 ms at a rate of 100 MSymbols/s. However, out of these, only round 10 ms correspond to quantum data and the rest are either synchronization signals or

other parts of the classical communication needed in order to execute the protocol. This limitation is mainly due to the memory available to store this data for its post-processing; for under 100 ms of data 1 GB of storage is necessary. In order to see the results of the atmospheric emulation during an entire satellite pass as depicted in figure 5.3a we will have to modify the software to perform multiple runs of the experiment and during each one using the VOA to emulate the attenuation of a different part of the trajectory. This sequential run of tests would either have to be stored in a high capacity hard drive or, alternatively, part of the DSP could be applied after each run in order to extract the quantum data: storing only the quantum data could significantly reduce the memory required.

An interesting addition to a future QKD demonstration with atmospheric channel emulation would be the implementation of a free-space turbulence simulator and a real adaptive optics bench. The PICOLO bench at ONERA [103], is a free-space turbulence emulator designed to represent a LEO-to-ground link at 10° elevation. It consists of a 1 m long bench composed of various mirrors, a spatial light modulator (SLM) and three rotating phase screens that were carefully etched in order to represent propagation over a specific turbulent volume. The turbulence represented corresponds to a Fried parameter r_0 of 2.6 cm, significantly more severe than any of the profiles we consider and likely too harsh for any QKD application. In order to make use of this free-space simulator it would be necessary to make some modifications so that the turbulence emulated is less severe. Detailed calculations would have to be made but removing one of the phase screens or changing their relative position could be an option to better adapt it to the atmospheric conditions we wish to represent. It is important to note, however, that this bench will only account for the effect of turbulence, path loss is not taken into account and the effect of AO correction would have to be tested by adding another experimental setup.

LISA [104] is an experimental adaptive optics bench designed at ONERA. It consists of a Shack-Hartmann wavefront sensor, a deformable mirror with magnetic actuators and controlled with a Linux computer. The sampling frequency of the feedback loop is 500 Hz, and it has a 2.2 frame delay in its current configuration. The system was shown to improve coupling into a single mode fiber on LEO satellite-to-ground optical links and could be an interesting addition to a more complex satellite-to-ground QKD experimental bench. At ONERA, efforts have already been made to couple the PICOLO and LISA benches, but further work is needed in order to adapt them for use in a QKD setting and additional emulation of path loss and beam wandering effects is necessary in order to fully represent a LEO-to-ground atmospheric channel.

5.2 Deformable lens experimental tests

The adaptive optics systems we have focused on so far, are currently the most widely used type of correction system, but they are not the only way to correct atmospheric turbulence induced effects. In the following we will examine the results of some experimental tests made with deformable lenses that were performed in collaboration with the adaptive optics team at the CNR-IFN laboratory in Padova.

The first alternative correction scheme we will analyze is depicted in figure 5.6. It consists of a lens that focuses the incoming beam, a tunable prism and a beam splitter that will divide the optical power with part of it going to a camera and the rest being focused into a single-mode fiber. The tunable prism is our corrective device. It consists of a few layers of glass, with a transparent dielectric gel inserted in between them. The uppermost glass layer, where the received beam arrives, is supported by three piezoelectric actuators whose movement allows the surface to change its inclination [105]. Both the camera and the lens' actuators are connected to a computer where the adaptive optics feedback loop is closed. The actuators will change the surface inclination allowing to control the direction of the beam in two orthogonal directions according to the measurements taken by the camera. The limited number of piezoelectric elements means that this device is only able to compensate tip-tilt and high order aberrations remain uncorrected.

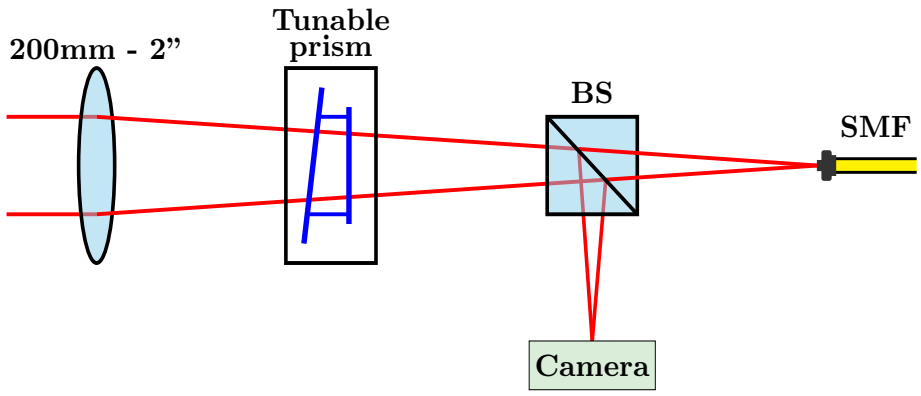
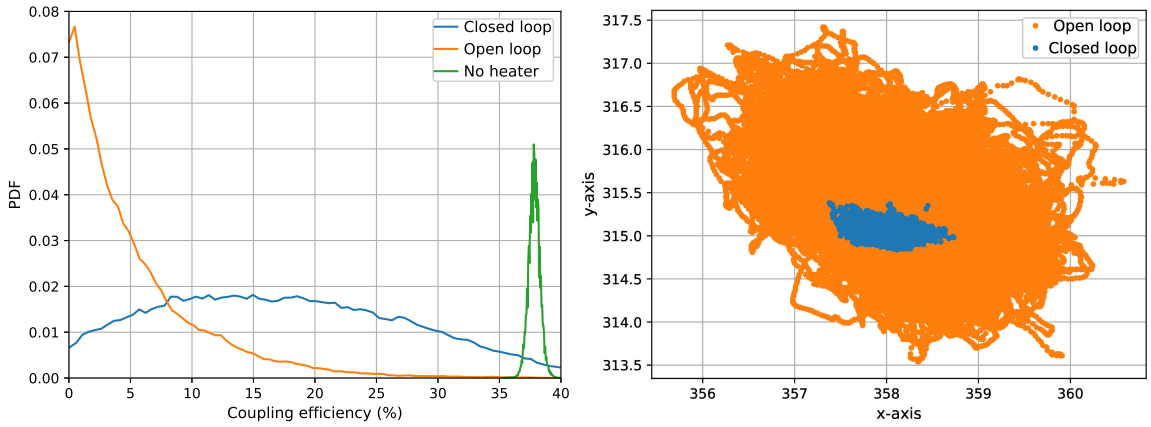


Figure 5.6: Receiver with tunable prism for Tip-Tilt compensation.

In order to test if this lens was capable of improving coupling into the optical fiber after atmospheric propagation we performed some tests in the CNR-IFN laboratory. The emitter consisted of a collimated beam from a telecom wavelength laser, and it was placed approximately one meter away from the receiver. The optical fiber was located in a support with manual control of the x and y axis and motorized control in the z-axis which allowed us to precisely align the received beam into its core. Since the test was performed indoors, we employed a small electrical hot plate, that was placed below the free-space link, in order to create some artificial turbulence effects and see

the response of the tunable prism. Figure 5.7 shows some results of this experiment.



(a) Coupling efficiency (b) Centroids

Figure 5.7: Measurement results for the tunable prism experimental test.

In order to estimate the coupling efficiency, we used a free-space optical power meter to measure the power received right in front of the fiber and compared it with the power measured inside the fiber after coupling. The measurements were taken with a data acquisition system working at 1 kHz during 300 seconds. In figure 5.7a we can observe the probability distribution of the coupling efficiency measured with the heater both in open loop and with the feedback loop closed, as well as a control measurement done in the absence of the heater. We can see that the coupling efficiency is very affected by the turbulence created by the heater, it passes from a very narrow distribution with 37.8% coupling in the control case to a widespread range of values and a mean coupling efficiency of only 5.3% with no correction. When the control loop is closed and the tip-tilt lens is actively correcting the average direction of the incoming beam, we can see an improvement of the coupling efficiency. Low efficiency values, while still possible, are less likely to occur and the mean coupling efficiency increases to 17.7%. Figure 5.7b illustrates the measurements from the camera, each sample represents the centroid of the incoming beam. We can observe that without correction the turbulence greatly affects the wandering of the beam which on the fiber side of the setup can mean that despite previous alignment, the beam is not landing on the fiber core and thus is not coupled. When the feedback loop is closed, we can observe that the lens actively manages to limit the wandering of the beam, it is still spread around its intended target but significantly less so. We can see that using this tunable lens allows for a slight improvement of the coupling efficiency but correcting only the tip and tilt modes is not enough in order to have an acceptable performance.

The second correction scheme explored is more complex because it can correct higher order aberrations, it can be found in figure 5.8. The correction device this time is a

multi-actuator lens (MAL). It is based on the same operating principle as the tunable prism, it consists of two thin pieces of glass in between which a transparent gel is injected. However, for the MAL there is a total of 18 piezoelectric actuators placed between the glass plates, allowing for the correction of up to 5 radial orders [106].

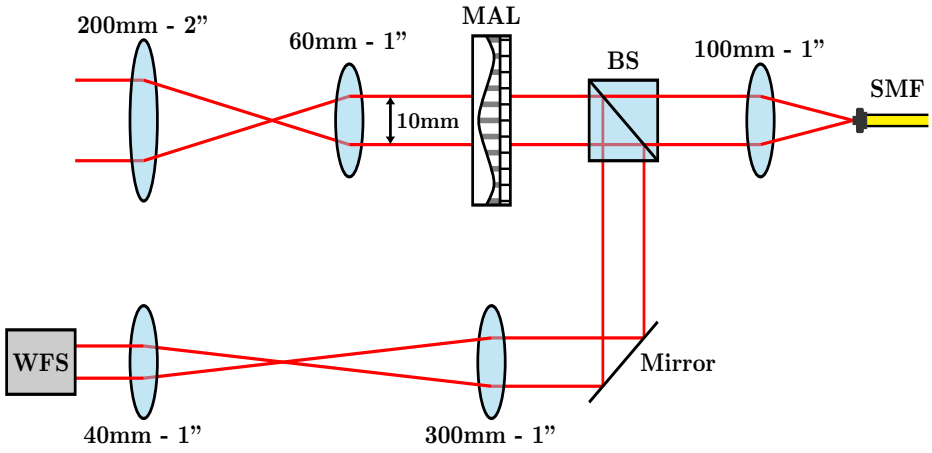


Figure 5.8: Receiver with multi-actuator lens for higher order compensation.

This new receiver consists of two lenses to refocus and then collimate the received beam which will then arrive to the MAL. The output of the deformable lens is divided in two, part of it will be coupled into the fiber with the help of an additional lens, and the rest will be redirected into a Shack-Hartmann wavefront sensor. The actuators of the lens will correct the received wavefront according to the aberrations measured by the wavefront sensor, which consists of a lenslet array and a camera with a 600 Hz sampling frequency. The transmitter is the same as the one used for the first experiment. In figure 5.9 we can observe the results of this demonstration. The receiver was once more placed 1 m away from the receiver and turbulence was emulated via the hotplate. Data acquisition was similar to the first setup, the sampling frequency of the acquisition card was 1 kHz and the measurements were taken during 300 seconds.

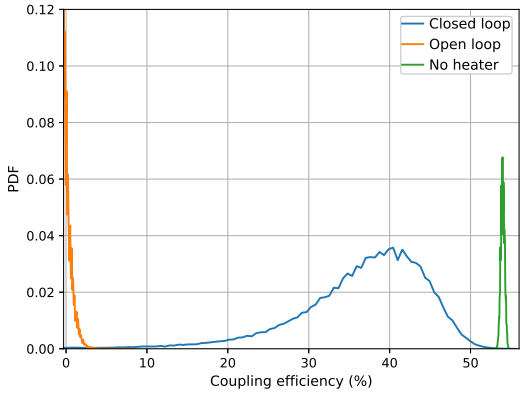
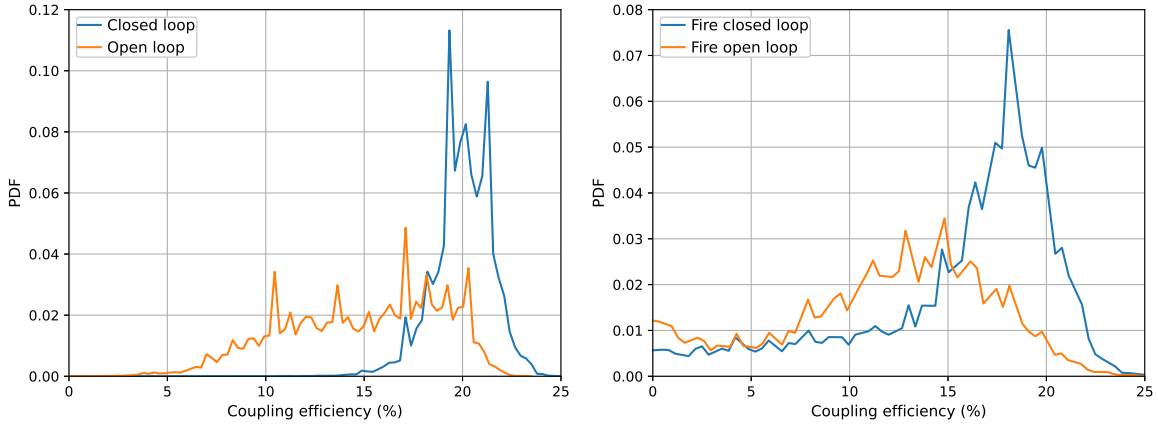


Figure 5.9: Measurement results for the multi-actuator lens experimental test.

In this case the coupling efficiency in the control case with no heater was a similarly narrow distribution, this time with an average coupling efficiency of 54%. The effect of the hotplate-induced turbulence is considerably more apparent in this experiment, the coupling efficiency distribution has a very steep exponential shape and the average coupling in the absence of correction is only around 0.26%. The impact of correction by the deformable lens is thus very significant. The coupling efficiency in the presence of turbulence when the control loop is closed increases to an average of 36.7%.

With the purpose of further testing the capabilities of this deformable lens, we performed an additional run of tests, this time on an empty field where we placed the transmitter and receiver at approximately a 50 m distance from each other. In figure 5.10 we can observe the probability distribution of this batch of measurements. For the first test, we measured the coupling efficiency with the unperturbed free-space link and for the second test, we lit a fire underneath the optical link in order to simulate stronger atmospheric effects with the help of the smoke and the increased temperature. As we can see, the behavior of the coupling efficiency in this longer link is more erratic. Nevertheless, we observe an improvement in the average coupling efficiency, in the unperturbed case the mean coupling efficiency increases from 14% to 20% and the standard deviation of the distribution is reduced from 4% to 1.5%. The effect is even more noticeable for the higher turbulence fire case, where the mean coupling increases from 7.8% to 14.5% and the standard deviation goes from 8% to 6.5%.



(a) Field test

(b) Field test with fire

Figure 5.10: Measurement results for the multi-actuator lens field test.

Further analysis of these experimental results is planned, this will be done in part by estimating the performance a QKD system would have when considering a free-space link like the one we tested. This will permit us to examine the effect this alternative correction scheme could have on the secret key rate and later on the experimental setup could be tested in conjunction with a QKD emitter qnd receiver pair.

5.3 Conclusion

We have described the last stages of our study in which we started developing an experimental setup in order to validate our simulation results. The challenges encountered during this process have been presented, as well as some possible solutions to be tried in order to overcome them. We present as well the results of an experimental bench aimed to analyze the impact of an alternative correction scheme on single-mode fiber coupling. This correction method is based on deformable lenses and the measurements show an improvement on the performance of the free-space link tested.

Chapter 6

Conclusions

The field of quantum cryptography and more generally, quantum communication has been the subject of very active research in the last few decades. Being able to communicate securely has been a topic of interest for a long time, but the increasing threat to our current classical cryptographic methods has pushed the rapid development of new solutions that guarantee higher levels of security.

The family of solutions we focused on throughout this manuscript, quantum key distribution (QKD), aims to ensure information-theoretic security of communication as opposed to the classical approach used in modern communication systems that relies on mathematical complexity and computational assumptions. Due to the quantum nature of the optical signal employed for key exchange, terrestrial implementations using fiber can only reach a limited distance, which is why we have decided to study the utilization of satellites in order to potentially establish long-distance QKD links at an intercontinental level.

Transmission of optical signals within a single-mode fiber has the issue of incurring in an exponential increase of losses with distance. The propagation losses of an atmospheric channel in contrast, increase quadratically. Nevertheless, satellite-to-ground communication links involve a new set of challenges to be taken into account such as turbulence effects, beam wandering, and the absorption and scattering effects of the atmosphere, several of which are dependent on geographical location and meteorological conditions. We decided to study how an adaptive optics system could help mitigate some of these effects via a feedback loop measuring and partially correcting the aberrations of the incoming wave.

We have shown a way to model the behavior of the atmospheric channel between a ground station and a low earth orbit satellite by taking into account the analytical descriptions of the aforementioned effects. We start by constructing day and nighttime turbulence profiles from measurements belonging to different databases. With these profiles and through a pseudo-analytic simulation tool, we estimated the effect

of certain turbulence conditions on the coupling efficiency of the optical signal into a single-mode fiber in the presence of adaptive optics correction.

We employed well established models found in the literature to calculate the geometrical losses affecting the propagated wave. We estimated as well the proportion of the emitter's divergent beam that was collected into a receiving aperture when taking into account beam wandering due to imperfect pointing. Through the modification of an existing simulation tool, we justified the hypothesis of independence of the turbulence and pointing jitter effects. Finally, we combined the coupling efficiency and beam wandering simulations at different elevations in order to obtain the probability distribution of the transmission efficiency of the channel for the entire visibility time of the satellite.

The final performance metric we focused on is the secret key rate which will depend on the transmission efficiency of the channel in various ways, according to the QKD protocol considered. Our simulation results have shown that for all three QKD protocols considered, two DV and one CV protocol, the use of an adaptive optics system capable of correcting high order aberrations of the signal received at the ground station, increased the coupling efficiency and therefore improved the overall final key rate.

This improvement is particularly significant in a daytime turbulence setting, where the key rate was found to be up to three orders of magnitude higher when considering an adaptive optics system capable of correcting 15 Zernike radial orders instead of the standard tip-tilt compensation scheme most ground stations are currently equipped with by default. Even in nighttime conditions, the use of an AO system is shown to extend the range of satellite altitudes at which a key exchange would be deemed feasible by a few hundred kilometers.

When extending the study to the entangled photon QKD protocol, we had to take into account the different visibility angles at which each of the ground stations was able to communicate with the satellite. In addition to the key rate, for this protocol we analyzed two intermediary metrics as well, the rate at which Alice and Bob had a coincidental detection and the quantum bit error rate (QBER).

We can observe that the use of AO has a significant impact on both of these values, the maximal coincidence rate goes from being of the order of 10^1 counts/s for a system correcting only first order aberrations to 10^3counts/s when considering a complex AO capable of correcting up to 15 or 20 radial orders. Concerning the QBER, it was significantly decreased, it went from being around 50% throughout the entire satellite visibility time, to remaining under 10% when using complex AO to correct for turbulence effects. The performance improvement is once again more significantly noticeable when computing the final key rate. Extracting a key is not deemed feasible at all when no correction or very low correction is considered, instead, an AO cor-

recting up to 15 radial orders is necessary for obtaining a key during daytime in both scenarios examined. In the simulations with high order AO it was estimated that up to 250 bits/s could be extracted in average by the two ground stations per satellite pass. These results expand upon existing experimental analysis like the one from the Micius satellite. We consider a different wavelength, and a larger applicability range due to our consideration of daytime operation.

Finally, we started taking steps towards an experimental validation of our simulation results. This was done employing two approaches: on one hand we started working towards the incorporation of an atmospheric channel emulator into an existing CV-QKD setup and on the other hand, we tested the performance of some alternative turbulence compensation schemes.

For the first approach, we managed to show a simple emulation of the atmospheric channel by using an electronic variable optical attenuator (VOA) to apply a time series of attenuation values that correspond to a specific turbulence scenario at a given satellite altitude. Nevertheless, there are some challenges for integrating this emulator with the current CV-QKD experimental bench present at LIP6. The original setup was not designed for operation at high attenuation and its excess noise is too high to obtain a positive key rate under those conditions. Further modification of both the hardware and the software of the setup is thus necessary in order to test our models. This may include changes to Alice's laser and Bob's DSP functions for example.

For the second experimental approach, we were able to test alternative turbulence correction methods involving deformable lenses, one of them a tunable prism capable of simple tip-tilt correction and the other a lens involving 18 piezoelectric actuators able to correct up to 5 radial orders. Through both in-lab experiments and a field test, we were able to show the increase in coupling efficiency by employing both lenses, with the improvement being more significant for the more complex lens. Through this we were able to show the potential usefulness of a compensation system different from traditional adaptive optics.

Perspectives

There are several ways in which the work we have presented in this manuscript could be expanded upon. The most direct would be by finalizing the in-lab validation we started to work towards, first with our simple VOA-based channel emulator and later on with a free-space atmospheric emulator such as the PICOLO bench and a real AO system like LISA, both systems currently present at ONERA.

Further work could also be developed on the network aspect of things, incorporating

atmospheric models to analysis of quantum networks involving satellite-to-ground links. We have started some preliminary work on this through the simulation of connection of quantum cities through satellite links [5]. This was done through the *Netsquid* simulation software and employing vastly simplified atmospheric channel models. The next step in this regard, involves using the more detailed channel model described in this manuscript in order to evaluate these network's performance.

Lastly, inclusion of other protocols is of interest as well, such as our current efforts to examine the feasibility of uplink twin-field QKD with a geostationary satellite, taking into account point-ahead angle compensation methods developed at ONERA. Modelling an uplink with a GEO satellite involves slightly different challenges than the previously analyzed downlink LEO scenario. Path loss is significantly higher but communication with it is not limited to the few minutes, once or twice per day visibility of LEO satellites.

The analysis detailed within this manuscript as well as the future work that can expand upon what we have done, can prove to be useful for the design and planning of real implementations of satellite-to-ground QKD.

Bibliography

[1] Valerio Scarani et al. "The security of practical quantum key distribution". *Rev. Mod. Phys.* 81 (2009), pp. 1301–1350. DOI: 10.1103/RevModPhys.81.1301. URL: https://link.aps.org/doi/10.1103/RevModPhys.81.1301.

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

[3] Daniele Dequal et al. "Feasibility of satellite-to-ground continuous-variable quantum key distribution". en. *npj Quantum Information* 7.1 (2021), p. 3. ISSN: 2056-6387. DOI: 10.1038/s41534-020-00336-4. URL: http://www.nature.com/articles/s41534-020-00336-4 (visited on 05/21/2021).

[4] Valentina Marulanda Acosta et al. *Analysis of satellite-to-ground quantum key distribution with adaptive optics*. 2021. arXiv: 2111.06747 [quant-ph].

[5] Raja Yehia et al. *Connecting Quantum Cities: Simulation of a Satellite-Based Quantum Network*. 2023. arXiv: 2307.11606 [quant-ph].

[6] Clifford C Cocks. "A note on non-secret encryption". *CESG Memo* (1973).

[7] Carl Pomerance. "A tale of two sieves". *Notices of the American Mathematical Society* 43.12 (1996), pp. 1473–1485.

[8] Gilbert S. Vernam. *Secret Signaling System*. Patent. US, 1919.

[9] Joan Daemen and Vincent Rijmen. *The design of Rijndael: AES — the Advanced Encryption Standard*. Springer-Verlag, 2002, p. 238. ISBN: 3-540-42580-2.

[10] *Algorithms for quantum computation: discrete logarithms and factoring*. 1994, pp. 124–134. DOI: 10.1109/SFCS.1994.365700.

[11] Lov K. Grover. "A Fast Quantum Mechanical Algorithm for Database Search". In: *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*. STOC '96. Philadelphia, Pennsylvania, USA: Association for Computing Machinery, 1996, pp. 212–219. ISBN: 0897917855. DOI: 10.1145/237814.237866.

[12] Ramona Wolf. *Quantum key distribution*. Springer, 2021.

[13] William K Wootters and Wojciech H Zurek. "A single quantum cannot be cloned". *Nature* 299.5886 (1982), pp. 802–803. DOI: 10.1038/299802a0.

[14] E. Schrödinger. "Discussion of Probability Relations between Separated Systems". *Mathematical Proceedings of the Cambridge Philosophical Society* 31.4 (1935), pp. 555–563. DOI: 10.1017/S0305004100013554.

[15] A. Einstein, B. Podolsky, and N. Rosen. "Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?" *Phys. Rev.* 47 (1935), pp. 777–780. DOI: 10.1103/PhysRev.47.777.

[16] John S Bell. "On the Einstein Podolsky Rosen paradox". *Physics Physique Fizika* 1.3 (1964), p. 195. DOI: 10.1103/PhysicsPhysiqueFizika.1.195.

[17] Stuart J. Freedman and John F. Clauser. "Experimental Test of Local Hidden-Variable Theories". *Phys. Rev. Lett.* 28 (1972), pp. 938–941. DOI: 10.1103/PhysRevLett.28.938.

[18] W. Heisenberg. "Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik". *Zeitschrift für Physik* (1927). DOI: 10.1007/BF01397280.

[19] A. Muller, J. Breguet, and N. Gisin. "Experimental Demonstration of Quantum Cryptography Using Polarized Photons in Optical Fibre over More than 1 km". *Europhysics Letters* 23.6 (1993), p. 383. DOI: 10.1209/0295-5075/23/6/001.

[20] Charles H. Bennett and Gilles Brassard. "Quantum cryptography: Public key distribution and coin tossing". *Theoretical Computer Science* 560 (2014). Theoretical Aspects of Quantum Cryptography – celebrating 30 years of BB84, pp. 7–11. ISSN: 0304-3975. DOI: 10.1016/j.tcs.2014.05.025.

[21] Alberto Carrasco-Casado, Veronica Marmol, and Natalia Denisenko. *Free-Space Quantum Key Distribution*. 2016, pp. 589–607. ISBN: 978-3-319-30200-3. DOI: 10.1007/978-3-319-30201-0_27.

[22] Hoi-Kwong Lo, Hoi Fung Chau, and Mohammed Ardehali. "Efficient quantum key distribution scheme and a proof of its unconditional security". *Journal of Cryptology* 18 (2005), pp. 133–165. DOI: 10.1007/s00145-004-0142-y.

[23] Xiang-Bin Wang. "Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography". *Phys. Rev. Lett.* 94 (2005), p. 230503. DOI: 10.1103/PhysRevLett.94.230503.

[24] Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen. "Decoy State Quantum Key Distribution". *Phys. Rev. Lett.* 94 (2005), p. 230504. DOI: 10.1103/PhysRevLett.94.230504.

[25] Charles Ci Wen Lim et al. "Concise security bounds for practical decoy-state quantum key distribution". *Physical Review A* 89.2 (2014), p. 022307. DOI: 10.1103/PhysRevA.89.022307.

[26] Charles H Bennett, Gilles Brassard, and N David Mermin. "Quantum cryptography without Bell's theorem". *Physical review letters* 68.5 (1992), p. 557. DOI: 10.1103/PhysRevLett.68.557.

[27] Morton H. Rubin et al. "Theory of two-photon entanglement in type-II optical parametric down-conversion". *Phys. Rev. A* 50 (1994), pp. 5122–5133. DOI: 10.1103/PhysRevA.50.5122.

[28] Xiongfeng Ma, Chi-Hang Fred Fung, and Hoi-Kwong Lo. "Quantum key distribution with entangled photon sources". *Physical Review A* 76.1 (2007), p. 012307. DOI: 10.1103/PhysRevA.76.012307.

[29] Pieter Kok and Samuel L. Braunstein. "Postselected versus nonpostselected quantum teleportation using parametric down-conversion". *Phys. Rev. A* 61 (2000), p. 042304. DOI: 10.1103/PhysRevA.61.042304.

[30] Marco Tomamichel et al. "Tight finite-key analysis for quantum cryptography". *Nature communications* 3.1 (2012), p. 634. DOI: 10.1038/ncomms1631.

[31] Juan Yin et al. "Entanglement-based secure quantum cryptography over 1,120 kilometres". *Nature* 582.7813 (2020), pp. 501–505. DOI: 10.1038/s41586-020-2401-y.

[32] Frédéric Grosshans and Philippe Grangier. "Continuous variable quantum cryptography using coherent states". *Physical review letters* 88.5 (2002), p. 057902. DOI: 10.1103/PhysRevLett.88.057902.

[33] Fabian Laudenbach et al. "Continuous-Variable Quantum Key Distribution with Gaussian Modulation—The Theory of Practical Implementations". *Advanced Quantum Technologies* 1.1 (2018), p. 1800011. DOI: 10.1002/qute.201800011.

[34] Igor Devetak and Andreas Winter. "Distillation of secret key and entanglement from quantum states". *Proceedings of the Royal Society A: Mathematical, Physical and engineering sciences* 461.2053 (2005), pp. 207–235. DOI: 10.1098/rspa.2004.1372.

[35] Simon Fossier et al. "Improvement of continuous-variable quantum key distribution systems by using optical preamplifiers". *Journal of Physics B: Atomic, Molecular and Optical Physics* 42.11 (2009), p. 114014. DOI: 10.1088/0953-4075/42/11/114014.

[36] Anthony Leverrier, Frédéric Grosshans, and Philippe Grangier. "Finite-size analysis of a continuous-variable quantum key distribution". *Phys. Rev. A* 81 (2010), p. 062343. DOI: 10.1103/PhysRevA.81.062343.

[37] Larry C Andrews. *Field guide to atmospheric optics*. 2019. DOI: 10.1117/3.2318080.

[38] AN Kolmogorov. "Local structure of turbulence in an incompressible viscous fluid at very high Reynolds numbers". *Soviet Physics Uspekhi* 10.6 (1968), p. 734. DOI: 10.1070/PU1968v010n06ABEH003710.

[39] George C. Valley. "Isoplanatic degradation of tilt correction and short-term imaging systems". *Appl. Opt.* 19.4 (1980), pp. 574–577. DOI: 10.1364/AO.19.000574.

[40] Jack L. Bufton. "Comparison of Vertical Profile Turbulence Structure with Stellar Observations". *Appl. Opt.* 12.8 (1973), pp. 1785–1793. DOI: 10.1364/AO.12.001785.

[41] D. L. Fried. "Optical Resolution Through a Randomly Inhomogeneous Medium for Very Long and Very Short Exposures". *J. Opt. Soc. Am.* 56.10 (1966), pp. 1372–1379. DOI: 10.1364/JOSA.56.001372.

[42] Thierry Fusco. "Correction partielle et anisoplanétisme en optique adaptative : traitements a posteriori et optique adaptative multiconjuguée". 2000NICE5442. PhD thesis. 2000, 307 p. URL: http://www.theses.fr/2000NICE5442.

[43] John W Hardy. *Adaptive optics for astronomical telescopes*. Vol. 16. Oxford Optical and Imaging Sci, 1998.

[44] Nicolas Vedrenne et al. "Performance analysis of an adaptive optics based optical feeder link ground station". In: *International Conference on Space Optics — ICSO 2020*. Vol. 11852. International Society for Optics and Photonics. SPIE, 2021, p. 1185219. DOI: 10.1117/12.2599232.

[45] J. Osborn et al. "Optical turbulence profiling with Stereo-SCIDAR for VLT and ELT". *Monthly Notices of the Royal Astronomical Society* 478.1 (2018), pp. 825–834. ISSN: 0035-8711, 1365-2966. DOI: 10.1093/mnras/sty1070. (Visited on 02/12/2021).

[46] Adolfo Comeron et al., eds. *Characterization of optical turbulence at the solar observatory at the Mount Teide, Tenerife*. 2013, p. 889015. DOI: 10.1117/12.2032744. (Visited on 06/17/2021).

[47] Héctor Vázquez Ramió et al. "European Extremely Large Telescope Site Characterization. II. High Angular Resolution Parameters". *Publications of the Astronomical Society of the Pacific* 124.918 (2012), pp. 868–884. ISSN: 00046280, 15383873. DOI: 10.1086/667599. (Visited on 09/21/2021).

[48] Nicolas A. Roddier. "Atmospheric wavefront simulation using Zernike polynomials". *Optical Engineering* 29.10 (1990), pp. 1174–1180. DOI: 10.1117/12.55712.

[49] Richard J Sasiela. *Electromagnetic wave propagation in turbulence: evaluation and application of Mellin transforms*. Vol. 18. Springer Science & Business Media, 2012.

[50] M. Gracheva and A. Lezhen. "Fluctuations in the intensity of light propagated through a medium with varying turbulence". *Soviet Radiophysics* (9(1) 1966), pp. 37–39.

[51] Stuart Shaklan and Francois Roddier. "Coupling starlight into single-mode fiber optics". *Appl. Opt.* 27.11 (1988), pp. 2334–2338. DOI: 10.1364/AO.27.002334.

[52] Bernard J. Klein and John J. Degnan. "Optical Antenna Gain. 1: Transmitting Antennas". *Appl. Opt.* 13.9 (1974), pp. 2134–2141. DOI: 10.1364/AO.13.002134.

[53] Robert K Tyson and Benjamin West Frazier. *Principles of adaptive optics*. CRC press, 2022.

[54] Aurélie Montmerle Bonnefois et al. "Feasibility demonstration of AO pre-compensation for GEO feeder links in a relevant environment". *Opt. Express* 30.26 (2022), pp. 47179–47198. DOI: 10.1364/OE.470705.

[55] Lucien Canuet et al. "Statistical properties of single-mode fiber coupling of satellite-to-ground laser links partially corrected by adaptive optics". *J. Opt. Soc. Am. A* 35 (2018), pp. 148–162. DOI: 10.1364/JOSAA.35.000148.

[56] Benoit Neichel. "Study of distant galaxies and tomographic adaptive optics for the elts". PhD thesis. Universite de Paris VII, 2008.

[57] Jean-Marc Conan. "Etude de la correction partielle en optique adaptative". 1994PA112450. PhD thesis. 1994, 343 P. URL: http://www.theses.fr/1994PA112450.

[58] Nicolas Védrenne et al. "Turbulence effects on bi-directional ground-to-satellite laser communication systems". In: *Proc. Int. Conf. Sp. Opt. Syst. Appl.* Vol. 12. 2012.

[59] D. Yu Vasylyev, A. A. Semenov, and W. Vogel. "Toward Global Quantum Communication: Beam Wandering Preserves Nonclassicality". *Phys. Rev. Lett.* 108.22 (2012), p. 220501. ISSN: 0031-9007. DOI: 10.1103/PhysRevLett.108.220501.

[60] Miguel Velez-Reyes and Fred A. Kruse, eds. *MODTRAN6: a major upgrade of the MODTRAN radiative transfer code*. Vol. 9088. International Society for Optics and Photonics. SPIE, 2014, 90880H. DOI: 10.1117/12.2050433.

[61] Jiu-Peng Chen et al. "Sending-or-Not-Sending with Independent Lasers: Secure Twin-Field Quantum Key Distribution over 509 km". *Phys. Rev. Lett.* 124 (7 2020), p. 070501. DOI: 10.1103/PhysRevLett.124.070501.

[62] Jiu-Peng Chen et al. "Twin-field quantum key distribution over a 511 km optical fibre linking two distant metropolitan areas". *Nature Photonics* 15.8 (2021), pp. 570–575. ISSN: 1749-4893. DOI: 10.1038/s41566-021-00828-5. URL: https://doi.org/10.1038/s41566-021-00828-5.

[63] Mirko Pittaluga et al. "600-km repeater-like quantum communications with dual-band stabilization". *Nature Photonics* 15.7 (2021).

[64] Yang Liu et al. "Experimental Twin-Field Quantum Key Distribution over 1000 km Fiber Distance". *Phys. Rev. Lett.* 130 (21 2023), p. 210801. DOI: 10.1103/PhysRevLett.130.210801. URL: https://link.aps.org/doi/10.1103/PhysRevLett.130.210801.

[65] Sheng-Kai Liao et al. "Satellite-Relayed Intercontinental Quantum Network". *Phys. Rev. Lett.* 120 (3 2018), p. 030501. DOI: 10.1103/PhysRevLett.120.030501. URL: https://link.aps.org/doi/10.1103/PhysRevLett.120.030501.

[66] D. Vasylyev, W. Vogel, and F. Moll. "Satellite-mediated quantum atmospheric links". *Phys. Rev. A* 99 (5 2019), p. 053830. DOI: 10.1103/PhysRevA.99.053830. URL: https://link.aps.org/doi/10.1103/PhysRevA.99.053830.

[67] S. Pirandola et al. "Advances in quantum cryptography". en. *Advances in Optics and Photonics* 12.4 (2020), p. 1012. ISSN: 1943-8206. DOI: 10.1364/AOP.361502. URL: https://www.osapublishing.org/abstract.cfm?URI=aop-12-4-1012 (visited on 06/18/2021).

[68] Shi-Yang Shen et al. "Free-space continuous-variable quantum key distribution of unidimensional Gaussian modulation using polarized coherent states in an urban environment". *Phys. Rev. A* 100 (1 2019), p. 012325. DOI: 10.1103/PhysRevA.100.012325. URL: https://link.aps.org/doi/10.1103/PhysRevA.100.012325.

[69] Shiyu Wang et al. "Atmospheric effects on continuous-variable quantum key distribution". *New J. Phys.* 20.8 (2018), p. 083037. ISSN: 1367-2630. DOI: 10.1088/1367-2630/aad9c4. URL: https://iopscience.iop.org/article/10.1088/1367-2630/aad9c4 (visited on 07/06/2019).

[70] László Ruppert et al. "Fading channel estimation for free-space continuous-variable secure quantum communication". *New J. Phys.* 21.12 (2019), p. 123036. ISSN: 1367-2630. DOI: 10.1088/1367-2630/ab5dd3. URL: https://iopscience.iop.org/article/10.1088/1367-2630/ab5dd3 (visited on 02/06/2020).

[71] Jasminder S Sidhu et al. "Finite key effects in satellite quantum key distribution". *npj Quantum Information* 8.1 (2022), p. 18.

[72] François Roddier. "Adaptive optics in astronomy" (1999).

[73] Mark T. Gruneisen et al. "Adaptive-Optics-Enabled Quantum Communication: A Technique for Daytime Space-To-Earth Links". *Phys. Rev. Appl.* 16 (1 2021), p. 014067. DOI: 10.1103/PhysRevApplied.16.014067. URL: https://link.aps.org/doi/10.1103/PhysRevApplied.16.014067.

[74] Mark T. Gruneisen et al. "Adaptive spatial filtering for daytime satellite quantum key distribution". In: *Proc. SPIE 9254, Emerging Technologies in Security and Defence II; and Quantum-Physics-based Information Security III*. Ed. by Mark T. Gruneisen et al. Amsterdam, Netherlands, 2014, p. 925404. DOI: 10.1117/12.2071278. URL: http://proceedings.spiedigitallibrary.org/proceeding.aspx?doi=10.1117/12.2071278 (visited on 06/18/2021).

[75] Mark T. Gruneisen, Michael B. Flanagan, and Brett A. Sickmiller. "Modeling satellite-Earth quantum channel downlinks with adaptive-optics coupling to single-mode fibers". *Optical Engineering* 56.12 (2017), p. 12611. ISSN: 0091-3286. DOI: 10.1117/1.OE.56.12.126111. URL: https://www.spiedigitallibrary.org/journals/optical-engineering/volume-56/issue-12/126111/Modeling-satellite-Earth-quantum-channel-downlinks-with-adaptive-optics-coupling/10.1117/1.OE.56.12.126111.full (visited on 06/18/2021).

[76] Michael D. Oliker and Mark T. Gruneisen. "How much value does adaptive optics add to a satellite QKD uplink?" In: *Quantum Technologies and Quantum Information Science V*. Ed. by Mark T. Gruneisen et al. Strasbourg, France: SPIE, 2019, p. 6. ISBN: 978-1-5106-3037-6 978-1-5106-3038-3. DOI: 10.1117/12.2537962. URL: https://www.spiedigitallibrary.org/conference-proceedings-of-spie/11167/2537962/How-much-value-does-adaptive-optics-add-to-a-satellite/10.1117/12.2537962.full (visited on 06/18/2021).

[77] Geng Chai et al. "Suppressing excess noise for atmospheric continuous-variable quantum key distribution via adaptive optics approach". *New Journal of Physics* 22.10 (2020), p. 103009. DOI: 10.1088/1367-2630/abb47c. URL: https://dx.doi.org/10.1088/1367-2630/abb47c.

[78] R. Nicholas Lanning et al. "Quantum Communication over Atmospheric Channels: A Framework for Optimizing Wavelength and Filtering". *Phys. Rev. Applied* 16 (4 2021), p. 044027. DOI: 10.1103/PhysRevApplied.16.044027. URL: https://link.aps.org/doi/10.1103/PhysRevApplied.16.044027.

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

[80] Sheng-Kai Liao et al. "Satellite-to-ground quantum key distribution". *Nature* 549.7670 (2017), pp. 43–47. ISSN: 0028-0836, 1476-4687. DOI: 10.1038/nature23655. URL: http://www.nature.com/doifinder/10.1038/nature23655 (visited on 01/15/2019).

[81] Cyril Petit et al. "FEELINGS : the ONERA's optical ground station for Geo Feeder links demonstration". In: *2022 IEEE International Conference on Space Optical Systems and Applications (ICSOS)*. 2022, pp. 255–260. DOI: 10.1109/ICSOS53063.2022.9749705.

[82] M. Avesani et al. "QCoSOne: a chip-based prototype for daylight free-space QKD at telecom wavelength". In: *Frontiers in Optics + Laser Science APS/DLS*. Optical Society of America, 2019, FTu6A.2. DOI: 10.1364/FIO.2019.FTu6A.2. URL: http://www.osapublishing.org/abstract.cfm?URI=FiO-2019-FTu6A.2.

[83] Luca Calderaro et al. "Towards quantum communication from global navigation satellite system". *Quantum Science and Technology* 4.1 (2018), p. 015012. DOI: 10.1088/2058-9565/aaefd4. URL: https://dx.doi.org/10.1088/2058-9565/aaefd4.

[84] F. X. Kneizys et al. *Users Guide to LOWTRAN 7*. Air Force Geophysics Laboratory. 16, 1988. 146 pp. URL: https://apps.dtic.mil/sti/citations/ADA206773.

[85] Alessia Scriminich et al. *Optimal design and performance evaluation of free-space Quantum Key Distribution systems*. 2021. DOI: 10.48550/ARXIV.2109.13886.

[86] Bing Qi et al. "Generating the local oscillator "locally" in continuous-variable quantum key distribution based on coherent detection". *Physical Review X* 5.4 (2015), p. 041009.

[87] Joseph W Goodman. *Statistical optics*. John Wiley & Sons, 2015.

[88] A. Le Kernec et al. "The H2020 VERTIGO project towards tbit/s optical feeder links". In: *International Conference on Space Optics — ICSO 2020*. Ed. by Bruno Cugny, Zoran Sodnik, and Nikos Karafolas. Vol. 11852. International Society for Optics and Photonics. SPIE, 2021, p. 1185217. DOI: 10.1117/12.2599229. URL: https://doi.org/10.1117/12.2599229.

[89] Ayan Biswas et al. "Use of Non-Maximal entangled state for free space BBM92 quantum key distribution protocol". *arXiv preprint arXiv:2307.02149* (2023).

[90] Ramniwas Meena, Subhashish Banerjee, et al. "Analysing QBER and secure key rate under various losses for satellite based free space QKD". *arXiv preprint arXiv:2308.01036* (2023).

[91] Christopher J. Pugh et al. *Advanced Optical Technologies* 9.5 (2020), pp. 263–273. DOI: doi:10.1515/aot-2020-0017. URL: https://doi.org/10.1515/aot-2020-0017.

[92] Sungeun Oh. "Entangled photon source for satellite-based QKD". In: *Photonics for Quantum 2023*. Ed. by Donald F. Figer and Michael Reimer. Vol. PC12633. International Society for Optics and Photonics. SPIE, 2023, PC1263302. DOI: 10.1117/12.2688372. URL: https://doi.org/10.1117/12.2688372.

[93] Yuan Cao et al. "Entanglement-based quantum key distribution with biased basis choice via free space". *Opt. Express* 21.22 (2013), pp. 27260–27268. DOI: 10.1364/OE.21.027260. URL: https://opg.optica.org/oe/abstract.cfm?URI=oe-21-22-27260.

[94] Matthew P Peloso et al. "Daylight operation of a free space, entanglement-based quantum key distribution system". *New Journal of Physics* 11.4 (2009), p. 045007.

[95] F Basso Basset et al. "Daylight entanglement-based quantum key distribution with a quantum dot source". *Quantum Science and Technology* 8.2 (2023), p. 025002.

[96] Nina Leonhard et al. "Protecting the entanglement of twisted photons by adaptive optics". *Phys. Rev. A* 97 (1 2018), p. 012321. DOI: 10.1103/PhysRevA.97.012321. URL: https://link.aps.org/doi/10.1103/PhysRevA.97.012321.

[97] John Gariano and Ivan B. Djordjevic. "SKR improvement for an entanglement assisted BB84 system using adaptive optics on an FSO link". In: *OSA Advanced Photonics Congress (AP) 2019 (IPR, Networks, NOMA, SPPCom, PVLED)*. Optica Publishing Group, 2019, QtW2E.4. DOI: 10.1364/SPPCOM.2019.QtW2E.4.

[98] Wenjun Wen et al. "Realizing an Entanglement-Based Multiuser Quantum Network with Integrated Photonics". *Phys. Rev. Appl.* 18 (2 2022), p. 024059. DOI: 10.1103/PhysRevApplied.18.024059.

[99] Thomas Paulet and Bryan Cazabonne. "An open-source solution for TLE based Orbit Determination". In: *8th European conference on space debris*. 2021.

[100] THORLABS. *V1550PA*. 2017. URL: https://www.thorlabs.com/_sd.cfm?fileName=TTN132794-S01.pdf&partNumber=V1550PA.

[101] Yoann Piétri et al. "CV-QKD Receiver Platform Based On A Silicon Photonic Integrated Circuit". In: *OFC 2023 (Optical Fiber Communication Conference)*. Technical Digest Series. San Diego, CA, United States, 2023. URL: https://hal.science/hal-04020567.

[102] Stefania Sesia, Issam Toufik, and Matthew Baker. "LTE–The UMTS Long Term Evolution" (2009).

[103] M.-T. Velluet et al. "PICOLO: turbulence simulator for adaptive optics systems assessment in the context of ground-satellite optical links". In: *Environmental Effects on Light Propagation and Adaptive Systems III*. Ed. by Karin Stein and Szymon Gladysz. Vol. 11532. International Society for Optics and Photonics. SPIE, 2020, p. 1153207. DOI: 10.1117/12.2573954. URL: https://doi.org/10.1117/12.2573954.

[104] CB Lim et al. "Single-mode fiber coupling for satellite-to-ground telecommunication links corrected by adaptive optics". In: *SF2A-2018: Proceedings of the Annual meeting of the French Society of Astronomy and Astrophysics*. 2018, p. Di.

[105] Kevin Campaci. "Tip-Tilt correction with Fast Refractive Modulator in a telescope". PhD thesis. UNIVERSITÀ DEGLI STUDI DI PADOVA, 2022.

[106] M. Quintavalla et al. "Adaptive optics on small astronomical telescope with multi-actuator adaptive lens". In: *Free-Space Laser Communication and Atmospheric Propagation XXX*. Ed. by Hamid Hemmati and Don M. Boroson. Vol. 10524. International Society for Optics and Photonics. SPIE, 2018, p. 1052414. DOI: 10.1117/12.2290061. URL: https://doi.org/10.1117/12.2290061.