Satellite-based links towards a global quantum network

Inaugural dissertation

for the attainment of the title of doctor
in the Faculty of Mathematics and Natural Sciences
at the Heinrich Heine University Düsseldorf

presented by

Carlo Liorni
from Viterbo, Italy

Düsseldorf, March 2021

from the institute for Theoretical Physics III
at the Heinrich Heine University Düsseldorf

Published by permission of the
Faculty of Mathematics and Natural Sciences at
Heinrich Heine University Düsseldorf

Supervisor: Prof. Dr. Dagmar Bruß
Co-supervisor: PD Dr. Hermann Kampermann

Date of the oral examination: 01.06.2021

Preface and Acknowledgement

This doctoral thesis reports the results obtained during my experience as a PhD student at Heinrich Heine University Düsseldorf. I declare under oath that I have produced my thesis independently and without any undue assistance by third parties under consideration of the 'Principles for the Safeguarding of Good Scientific Practice at Heinrich Heine University Düsseldorf'.

I would like to thank my supervisors Prof. Dr. Dagmar Bruß and PD Dr. Hermann Kampermann for making me a better scientist. Most of all, I thank my family and my girlfriend for the constant support and for making me a better person.

Carlo Liorni
Düsseldorf
March 2021

Abstract

Quantum technologies have the potential to achieve revolutionary improvements over current classical technologies. The technical challenges that they introduce, however, make their translation from laboratories to real-life applications very arduous. For this reason, a thorough theoretical analysis of what can be achieved by quantum technologies, in the ideal case and in applications in the field, is mandatory.

This thesis deals with satellite-based quantum key distribution. In this recently developed research field, optical links between satellites and stations on the ground are used to share quantum information by means of faint beams of light. Such information, through specific protocols, can then be turned into a secret key shared between the communicating parties. This resource is of great value in today's world, since most of the information shared on the internet is encrypted. As we briefly introduce in the following paragraphs, three main aspects of satellite-based quantum communication are addressed in this thesis, all of great interest for the development of the field.

Satellite-based links, like any other atmospheric optical channel, are heavily influenced by the weather condition. This problem is well known since decades in classical communication but the peculiarities of quantum signal exchange calls for additional studies. We discuss how to model such links using modern techniques and study their performance in different weather conditions.

The usual assumption of an all-powerful adversary in quantum cryptography is very general but also unreasonably over-pessimistic in some cases. We studied techniques to bound the efficiency with which an adversary can tamper on a satellite-based quantum channel and analysed how this information can lead to higher rates in a cryptographic protocol.

The feasibility and effectiveness of satellite-to-ground quantum key distribution have been experimentally proven, but the potential of this technology goes far beyond that.

We present and study a satellite-based scheme to distribute entanglement over global distances, by means of quantum repeaters, using a small number of intermediate nodes. Such configurations might be a candidate building block for a future global quantum network.

The promising field of satellite quantum communication is attracting enormous interest in universities and institutions. The integration of satellite links with metropolitan fibre-based networks can be envisaged to represent the backbone of the future quantum internet.

Zusammenfassung

Quanten Technologien haben das Potenzial revolutionäre Verbesserungen über derzeitige klassische Technologien zu erzielen. Die technischen Herausforderungen, die mit ihnen einher gehen, machen ihre Übersetzung aus dem Labor hin zu echten Anwendungen jedoch sehr mühsam. Aus diesem Grund ist eine gründliche theoretische Analyse von dem, was mit Quanten Technologien erzielt werden kann, sowohl im Idealfall als auch in Anwendungen vor Ort, zwingend erforderlich.

Diese Doktorarbeit beschäftigt sich mit Satelliten-basierter Quantenverschlüsselung. In diesem kürzlich entwickeltem Forschungsfeld werden optische Verbindungen zwischen Satelliten und Bodenstationen benutzt um Quanteninformation mittels schwacher Lichtstrahlen zu verteilen. Solche Information kann, durch spezifische Protokolle, in einen geheimen und an alle Partien verteilten Schlüssel umgewandelt werden. Diese Resource ist heutzutage sehr wertvoll, da die meiste Information, die über das Internet verteilt wird, verschlüsselt ist. Wie wir in den folgenden Paragraphen kurz erläutern, werden drei Hauptaspekte der Satelliten-basierten Quantenkommunikation in dieser Doktorarbeit angesprochen, alle von großem Interesse für die Weiterentwicklung des Felds.

Satelliten-basierte Verbindungen werden, wie jeder andere athmosphärische optische Kanal, stark durch Wetterbedingungen beeinflusst. Dieses Problem ist seit Jahrzehnten in der klassischen Kommunikation wohlbekannt, aber die Eigenheiten eines Quantensignalaustauschs fordern weitere Studien. Wir diskutieren wie solche Verbindungen unter Verwendung moderner Techniken modelliert werden können, und erforschen ihre Leistung in verschiedenen Wetterbedingungen.

Die üblichen Annahme eines allmächtigen Gegenspielers in der Quantenverschlüsselung ist sehr allgemein, aber in manchen Fällen auch ungerechtfertigt übermäßig pessimistisch. Wir studieren Techniken um die Effizienz,

mit der ein Gegenspieler einen Satelliten-basierten Quantenkanal manipulieren kann, abzuschätzen und analysieren wie diese Information zu höheren Raten in kryptographischen Protokollen führen kann.

Die Umsetzbarkeit und Effizienz von Satelliten-zu-Boden Quantenverschlüsselung wurde experimentell demonstriert, aber das Potential dieser Technologie geht weit darüber hinaus. Wir präsentieren und studieren einen Satelliten-basierten Plan, um Verschränkung mittels Quantenrepeatern über globale Distanzen zu verteilen, wobei eine kleine Zahl vermittelnder Knoten benutzt wird. Solche Konfigurationen könnten ein Kandidat für Bausteine eines zukünftigen globalen Quantennetzwerks sein.

Das vielverprechende Feld der Satelliten-basierten Quantenkommunikation zieht enormes Interesse an Universitäten und Institutionen auf sich. Die Integration Satelliten-basierter Verbindungen mit städtischen faserbasierten Netzwerken kann als Rückgrat des zukünftigen Quanteninternets in Betracht gezogen werden.

Contents

Introduction 1

Quantum technologies are attracting more and more interest not only in the scientific landscape, but also in industry and among mass-media. They promise to revolutionize the field of computation [1, 2, 3], with devices able to solve very efficiently problems which are too complex for standard classical computers. Quantum protocols have the potential to improve the efficiency of our communication network. True and long-lasting information security can be achieved by means of the integration of classical and quantum protocols [4, 5]. More accurate and efficient measurements of any physical quantity can be achieved using quantum metrology procedures [6, 7, 8]. The potential of quantum technologies is enormous, given the extremely wide scope of possible applications.

However, as it constantly happens in the history of humanity, progress comes at a price. The advancement of our computational capabilities might endanger the foundations of our global communication system. As discussed in Chap. 3, nowadays most of our communications on the internet is based on public key encryp-

tion. The security of such schemes has its roots in the conjecture that some mathematical problems are inherently *hard* to solve. More precisely, it has been conjectured that the resources necessary to solve these problems scale exponentially with the size of the input. While the conjecture apparently holds true in the classical scenario, since no efficient protocols have been devised despite the huge commitment, it might not be true anymore in the realm of quantum computation. The most renown breakthrough is the proposal of a quantum algorithm by P. Shor [9], which solves problems like the factorization of very large numbers and the discrete logarithm in polynomial time. Such advancements threaten to undermine the validity of the conjecture above mentioned, so a different approach for proving secrecy and security need to be devised. One possible path is to modify the already known public key encryption schemes, exploiting problems which are conjectured to be computationally hard even in the quantum case. This is the goal of *post-quantum cryptography*. Otherwise, an inherently quantum cryptographic primitive can be introduced, namely, *Quantum Key Distribution* (QKD) [10]. The protocols in this family allow to distribute among two or more parties a secret key that can be utilized for encryption. As discussed in more detail in Chap. 3, the security of this key can be proven in an information-theoretic manner against an all-powerful eavesdropper, bounded only by the laws of quantum mechanics. This is much more general than the assumption of a computationally-bound adversary used in the classical case with public key encryption.

Quantum cryptography can be considered the field in quantum technologies that is in the most advanced state right now. Our grasp on its theoretical foundations and implications is solid and extensive. Many implementations have already been commercialized and more and more companies are entering the market. This is in stark contrast with other quantum technologies, which are still in the development stage and will likely stay in such state for several years. True quantum computation, for example,

has only been achieved on a very small scale, due to the significantly harsher technical requirement, despite the important economic commitment of many institutions and companies around the world.

1.1 Motivation of the work and brief overview of the results

Quantum protocols, on paper, seem to promise revolutionary improvements in almost every field of science and technology. The additional technical difficulties with respect to their classical counterparts, however, totally hinder their real-life applications in many cases. In this thesis, the main adversary of quantum technologies that we are going to confront is the loss of signals. Naturally, this problem is not exclusive to quantum devices: classical signals, for example in radio-frequency or optical communication, undergo the same process of loss. Such classical signals, however, can be amplified and replicated in order to counteract the effect of losses. It can be proven, on the other hand, that it is impossible to clone a generic quantum signal without introducing noise [11], which eventually destroys its advantage over classical resources. This problem is further discussed in Chap. 3, where we also show how this prerogative of quantum information can be used at our advantage.

The most natural solution for carrying quantum signals is, like in the classical case, encoding them into different states of light at different wavelengths. Nowadays the standard channel for high-rate optical communication is represented by optical fibres, the backbone of the global communication system as we experience it every day. The losses inside such waveguides are due to scattering and absorption and they grow exponentially with the distance travelled. This scaling makes it very difficult and inefficient to exchange quantum signals over distances longer than 100km. As discussed more in detail in Sec. 3.5, the current record dis-

tance for quantum key distribution in fibre is around 400km in laboratory, with extremely low key rates. The pursue of higher key rates over longer distances is one of the motivation for the introduction of satellite-based links for quantum communication [12, 13, 14, 15], that are the main topic of this thesis. In this case the quantum signals are exchanged by means of light beams sent through free-space from a transmitter telescope and collected by a receiver aperture. The two terminals can be either on satellites or on the ground. As thoroughly discussed in Chap. 4, satellite-based quantum communication has inherent advantages over the optical fibre implementation. A much more advantageous scaling of the loss with the distance can be achieved in some cases, since most of the propagation of the light happens in vacuum, outside the atmosphere.

However, such free-space atmospheric links are strongly influenced by the weather. Modelling the propagation of light beams through turbulent media, such as the atmosphere, is a very complex problem. In the last decades, this topic has been addressed regarding classical communication in the radio and visible parts of the electromagnetic spectrum [16]. The propagation of quantum light in such conditions necessitates additional study and this motivated our contribution, published as [17], discussed in Chap. 4 and attached to this thesis (Chap. 9). There, a modern model for quantum light propagation through atmospheric channels is generalized to the case of a non-uniform link. The results are then applied to study satellite-to-ground links (downlinks) and ground-to-satellite links (uplinks). The ability to take into account absorption in the atmosphere, turbulence effects and scattering on particulate (fog, haze, rain) allows to model the weather variations. The performance of such channels is then estimated in terms of the transmittance for different weather conditions. Finally, this result is used to assess the expected key rate of a QKD protocol over such channels.

Free-space optical links are physically inherently different from fibre-based channels. Consequently, some of the assumptions

that seem so natural in the latter case might need to be re-evaluated in the former. One example is the standard assumption of an all-powerful eavesdropper. Such an adversary can interact with the quantum channel in any way allowed by the laws of quantum mechanics. In satellite-based channels the adversary, in order to collect the light sent by the transmitter and interact with the receiver efficiently, would need very large telescopes, on a very large spacecraft. The parties should be able to spot such a presence on the line-of-sight between them. In a publication currently in preparation, we tackle the problem of bounding the efficiency with which the eavesdropper can tamper with the quantum channel, using monitoring techniques like RADAR or LIDAR. We also estimate what advantage in terms of key rate can be obtained when such bounded eavesdropper is assumed.

We finally address the problem of entanglement distribution over global distances. As already said, direct fibre links can only go as far as few hundred kilometres. Quantum repeaters have been proposed to enlarge the range of the entanglement distribution [18, 19]. A large number of intermediate nodes are necessary on the ground to achieve global distances, which in turn require quantum devices of extremely high quality. The use of satellite links to substitute fibre links may allow to reach global distances with a smaller number of nodes. In [20] we propose and analyse a scheme based on quantum repeaters and inter-satellite links. More details can be found in Chap. 7 and the paper is attached in Chap. 9. We compare the performance of the scheme with other solutions and discuss its implementation.

The results are further discussed in the corresponding sections of this thesis, Sec. 4.3, Sec. 5.1 and Sec. 7.1.

1.2 Structure of the thesis

The thesis is organized as follows. The main concepts regarding quantum states and quantum operations are introduced in

Chap. 2. There we also discuss some aspects of quantum information theory that will have a central role in the remainder of the thesis. In Chap. 3 we introduce QKD as the prominent Quantum Information application studied in this work. Satellite-based links for QKD, the main topic of the thesis, are addressed in Chap. 4. After a short review of the recent experimental efforts in the field, we tackle the problem of modelling such links and studying their performance. Chap. 5 is devoted to the study of realistic threat models tailored around the peculiarities of satellite-based quantum communication links. In particular we assume that additional channel monitoring techniques are used to bound how efficiently the eavesdropper can tamper with the communication between the trusted parties. In Chap. 6 we introduce the important concept of *Quantum Repeater* (QR), that allows to overcome distance limitations by the use of intermediate nodes able to perform quantum operations. We show in Chap. 7 how QRs combined with satellite-based channels could allow to distribute entanglement over global distances, well beyond what is achievable in ground implementations. The contribution of the author to the related publications is specified in Chap. 8. Further discussion takes place in Chap. 9, together with an outlook on possible future developments.

Elements of Quantum Information Theory 2

In this chapter we are going to introduce the basic concepts of *Quantum Information Theory* (QIT) that are necessary for the remainder of the thesis. What is a quantum state? What is a quantum operation? What is, roughly, the structure of the state space of a bi-partite quantum system? What is the quantum resource that goes under the name of entanglement? These are some of the questions that will be answered in this chapter. More details can be found in well-known books about quantum information theory, like [21] and [22]. In particular, we start by presenting the description of states in quantum mechanics (Sec. 2.1). We then describe how quantum operations act on them in Sec. 2.2. Finally, in Sec. 2.3, the concepts of quantum correlations and entanglement are briefly analysed.

2.1 States in quantum mechanics

A state of a physical system contains all the information available about the actual configuration of the system that one has obtained through measurements. Associated with a quantum system is a complex Hilbert space with scalar product $\langle \cdot, \cdot \rangle$ and corresponding norm $|| \cdot ||$. A *pure state*, associated with a state vector $|\psi\rangle$ in the Hilbert space satisfying $||\psi|| = 1$, describes a quantum system for which one has maximal information about its configuration. In other words, one has performed a preparation of the quantum system such that the values of a complete set of observables have been fixed. The state vector $|\psi\rangle$ is uniquely determined except for a global phase factor and the state itself corresponds to the associated *unity ray* $\{e^{i\phi} |\psi\rangle \, | \phi \in \mathbb{R}\}$.

The most elementary quantum system is the two-level system, associated to a two-dimensional Hilbert space $\mathbb{C}^2$. The basis elements of such vector space can be labelled $|0\rangle$ and $|1\rangle$. Any unit vector in this Hilbert space is of the form

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

where $\alpha, \beta \in \mathbb{C}$ and $|\alpha|^2 + |\beta|^2 = 1$. According to Eq. 2.1, the state of the system can correspond to $|0\rangle$ and $|1\rangle$ but it can also, crucially, occur in a coherent superposition of them. This extremely simple quantum system is of major importance in quantum information theory, where it is called quantum bit or *qubit*. It represents, in fact, the fundamental carrier of information in a quantum information processing device.

If one wants to include the possibility of partial information about the state of a system, unit rays are not a sufficient description any longer. The concept of *mixed state* incorporates ignorance about the preparation stage or as a result of an operation on the state. For example, in a beam of unpolarized spin-1/2 particles, the quantum state is given by the classical mixture with uniform distribution of particles in the unit rays of $|0\rangle$ and $|1\rangle$.

Another example of a mixed quantum state can be prepared using a classical random number generator. If it produces the output 1, which happens with probability p_1, the experimenter prepares the pure state $|\psi_1\rangle$. If the output is 2, with probability p_2 (with $p_1 + p_2 = 1$) the state $|\psi_2\rangle$ is generated. This procedure results in the production of the mixed state

$$\rho = p_1 |\psi_1\rangle \langle\psi_1| + p_2 |\psi_2\rangle \langle\psi_2| \ . \tag{2.2}$$

From now on, the state of a quantum mechanical system with Hilbert space $\mathcal{H}$ will be identified with a bounded operator ρ. It must also fulfil three requirements: 1) ρ is Hermitian or self-adjoint, $\rho = \rho^\dagger$, 2) it is a positive semi-definite operator $\rho \geq 0$ and 3) $\mathrm{Tr}[\rho] = 1$ due to the condition on the probabilities $\sum_{i=1}^{n} p_i = 1$. Furthermore, a state ρ is pure if $\rho^2 = \rho$ and mixed otherwise. For a given Hilbert space, the associated set of all possible states is denoted by $\mathcal{S}(\mathcal{H})$ and referred to as *state space*. The example above regarding the random number generator highlights a crucial property of the state space: its convexity. If ρ_1 and ρ_2 are elements of $\mathcal{S}(\mathcal{H})$, the same is true for all the states on the segment connecting them, $a\rho_1 + (1-a)\rho_2 \ , a \in [0,1]$. The convex combination corresponds to the mixing of two preparing procedures, ρ_1 with probability a and ρ_2 with probability $1-a$, ignoring then the information about which preparation was actually chosen. The extreme points in the convex state space are just one dimensional projectors $|\psi\rangle \langle\psi|$ with $||\psi|| = 1$.

On the other hand, any mixed state ρ admits a representation of the form

$$\rho = \sum_{i=1}^{n} p_i |\psi_i\rangle \langle\psi_i| \tag{2.3}$$

with a probability distribution $p_1, ..., p_n$ and projectors $|\psi_i\rangle \langle\psi_i|$, $i = 1, ..., n$.

A very convenient and effective way to describe the state of a qubit is the so-called *Bloch sphere representation*. As expressed in

Eq. 2.1, the coefficient of each of the two basis vector is a complex number. This means that the state is described by four real numbers. Only the relative phase between the coefficients of the two basis vectors has any physical meaning, however, so there is redundancy in this description. We can take the coefficient of $|0\rangle$ to be real and non-negative. This allows the state to be described by only three real numbers, giving rise to the three dimensions of the Bloch sphere, pictured in Fig. 2.1. The state of a pure quantum state can be described by just two parameters, for example the angles θ and ϕ in Fig. 2.1

$$|\psi\rangle = \cos(\theta/2)\,|0\rangle + e^{i\phi}\sin(\theta/2)\,|1\rangle \ , \tag{2.4}$$

with $0 \leq \theta \leq \pi$ and $0 \leq \phi \leq 2\pi$. So, the pure states belong to the surface of the sphere.

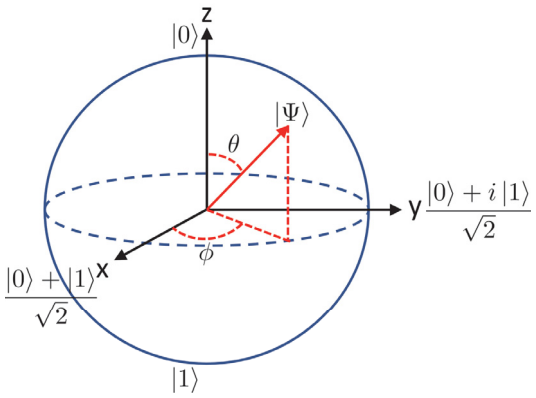

Figure 2.1: Bloch sphere representation of the state of a single qubit. The angles θ and ϕ completely describe a pure state, the modulus of the Bloch vector is also needed to describe a mixed state.

A more general mixed state is written as

$$\rho = \frac{1}{2}\left(\mathcal{I} + \vec{a}\vec{\sigma}\right) , \tag{2.5}$$

where $\mathcal{I}$ is the completely mixed state, at the centre of the Bloch sphere. The vector $\vec{a}$ is the so-called Bloch vector, the position in the sphere describing the state ρ. $\vec{\sigma}$ is the vector of the three Pauli matrices, described in Sec. 2.2.

We define now the *fidelity* between two quantum states, that will find great use in the remainder of the thesis. It is a measure of how *close* or indistinguishable they are. For the simple case of two pure states $|\psi\rangle$ and $|\phi\rangle$, it can be expressed as the modulus squared of the overlap between them

$$F(|\psi\rangle , |\phi\rangle) = |\langle\psi|\phi\rangle|^2 . \tag{2.6}$$

For mixed states ρ and σ, instead, the expression is the following

$$F(\rho, \sigma) = \left(\mathrm{tr}\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}\right)^2 , \tag{2.7}$$

where, for a positive semidefinite matrix M, $\sqrt{M}$ denotes its unique positive square root [21].

Many interesting phenomena arise in the case of a *composite* quantum system. The Hilbert space corresponding to a system composed of two parts (named A and B) is appropriately constructed as the *tensor product* of the Hilbert spaces of the subsystems,

$$\mathcal{H} = \mathcal{H}_\mathcal{A} \otimes \mathcal{H}_\mathcal{B} . \tag{2.8}$$

Let us consider finite-dimensional Hilbert spaces of dimension $N = \dim[\mathcal{H}_\mathcal{A}]$ and $M = \dim[\mathcal{H}_\mathcal{B}]$. If $\{|1\rangle_A , ..., |N\rangle_A\}$ is a basis of $\mathcal{H}_\mathcal{A}$ and $\{|1\rangle_B , ..., |M\rangle_B\}$ is a basis of $\mathcal{H}_\mathcal{B}$, then $\{|i\rangle_A \otimes |j\rangle_B | i = 1, ..., N; j = 1, ..., M\}$ is a basis of $\mathcal{H}$. A *product state vector* is a vector in the form

$$|\psi\rangle = |\phi\rangle_A \otimes |\phi\rangle_B = \left(\sum_{i=1}^{N} \alpha_i |i\rangle_A \right) \otimes \left(\sum_{j=1}^{M} \beta_j |j\rangle_B \right) \quad (2.9)$$

with complex coefficients α_i and β_j such that $\sum_{i=1}^{N} |\alpha_i| = 1$ and $\sum_{j=1}^{M} |\beta_j| = 1$. We will come back to product states in section 2.3, where we tackle the concepts of separability and entanglement.

A powerful tool in this context is the *Schmidt decomposition* [23] for pure states of bi-partite systems. Let $\mathcal{H} = \mathcal{H}_\mathcal{A} \otimes \mathcal{H}_\mathcal{B}$, $\mathcal{H}_\mathcal{A} = \mathcal{H}_\mathcal{B} = \mathbb{C}^N$ and $|\phi\rangle \in \mathcal{H}$ be a state vector. There exist an orthonormal basis $\{|1\rangle_A, ..., |N\rangle_A\}$ of $\mathcal{H}_\mathcal{A}$ and an orthonormal basis $\{|1\rangle_B, ..., |N\rangle_B\}$ of $\mathcal{H}_\mathcal{B}$ such that

$$|\psi\rangle = \sum_{i=1}^{N} \sqrt{\alpha_i} |i\rangle_A |i\rangle_B \ . \quad (2.10)$$

Here $\alpha_i, i = 1, ..., N$ are the so-called *Schmidt coefficients* of the decomposition, real positive numbers such that $\sum_{i=1}^{N} \alpha_i = 1$. The number of non-vanishing Schmidt coefficients takes the name of *Schmidt rank*.

2.2 Quantum Operations

Isolated quantum systems evolve as described by the *Schrödinger equation*. The time evolution of a quantum system with associated Hilbert space $\mathcal{H}$ corresponds to the unitary *dynamical map*

$$\rho \to \sigma = U \rho U^\dagger \ , \quad (2.11)$$

where $U : \mathcal{H} \to \mathcal{H}$ is a time-dependent unitary operator.

Another crucial mechanism that alters the state of a quantum system is the process of *measurement*. Let $i = 1, ..., K$ label possible outcomes of a measurement. Each outcome is associated with a projector π_i

$$\pi_i \pi_j = \delta_{ij} \pi_i \ , \quad \sum_{i=1}^{K} \pi_i = \mathbb{I} \ . \tag{2.12}$$

The state ρ of the system is changed by the measurement according to

$$\rho \to \sigma_i = \frac{\pi_i \rho \pi_i}{\mathrm{Tr}[\pi_i \rho \pi_i]} \ , \tag{2.13}$$

if outcome i was measured.

The outcome i is obtained with probability $p_i = \mathrm{Tr}[\pi_i \rho]$. This is what we refer to as *selective projective measurement*. A *non-selective projective map* corresponds to the map

$$\rho \to \sum_{i=1}^{K} \pi_i \rho \pi_i \ , \tag{2.14}$$

where the information about which outcome occurred is neglected.

A general definition of quantum operation can be formulated with the following axiomatic approach. Consider all the possible maps $\mathcal{E} : \mathcal{S}(\mathcal{H}) \to \mathcal{S}(\mathcal{H}')$ which are consistent with the statistical interpretation of quantum mechanics. $\mathcal{E}$ must be linear, to respect convex combinations of states discussed previously. In order to preserve the positive semi-definiteness of the quantum states, one also requires the map $\mathcal{E}$ to be *completely positive*. $\mathcal{E}$ is called completely positive if $\mathcal{E} \otimes \mathbb{I}_N$ is a positive map for all $N \in \mathbb{N}$. All such operations, that include unitary operations, non-selective projective measurements, appending of uncorrelated ancillae, dismissal of parts of a compound system and their combination, can be cast into the form

$$\rho \to \mathcal{E}(\rho) = \sum_{i=1}^{K} E_i \rho E_i^\dagger \ , \tag{2.15}$$

where the so-called *Kraus operators* $E_i : \mathcal{H} \to \mathcal{H}, i = 1, ..., K$ are not necessarily Hermitian. $\mathcal{E}$ is also *trace preserving* if the Kraus operators satisfy

$$\sum_{i=1}^{K} E_i^\dagger E_i = \mathbb{I}\,, \tag{2.16}$$

because it implies that $\sum_{i=1}^{K} \mathrm{Tr}[E_i \rho E_i^\dagger] = \mathrm{Tr}[\rho] = 1$.

Every trace-preserving quantum operation can be realized by appending an appropriate ancilla to the system, applying a joint unitary operation on the composite system and finally tracing out the ancilla. This concept is formalized in the so-called *Stinespring dilation theorem:* let $\mathcal{H}$ be a Hilbert space with dimension $\dim[\mathcal{H}] = N$ and let $\mathcal{E} : \mathcal{S}(\mathcal{H}) \to \mathcal{S}(\mathcal{H})$ be a trace-preserving quantum operation. Then there exists a Hilbert space $\mathcal{K}$ with $\dim[K] < N^2$ and, for any fixed $|\psi\rangle \in \mathcal{K}$, there exists a unitary operator $U : \mathcal{H} \otimes \mathcal{K} \to \mathcal{H} \otimes \mathcal{K}$ such that

$$\mathcal{E}(\rho) = \mathrm{Tr}_{\mathcal{K}}\big[U\big(\rho \otimes |\psi\rangle\langle\psi|\big)U^\dagger\big]\,. \tag{2.17}$$

2.2.1 Pauli matrices

The Pauli matrices are a set of three 2×2 complex, Hermitian and unitary matrices. They are extremely useful in quantum information theory and can be expressed as

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\,. \tag{2.18}$$

Together with the identity matrix $\mathcal{I}$ they form a basis for the real vector space of 2×2 Hermitian matrices. Since Hermitian operators represent observables in quantum mechanics, the Pauli matrices with the identity span the space of observables on a single qubit. The Pauli vector, referred to in Sec. 2.1, is defined as

$$\vec{\sigma} = \sigma_x \hat{x} + \sigma_y \hat{y} + \sigma_z \hat{z} \tag{2.19}$$

2.3 Quantum correlations and entanglement

Assume a bipartite quantum state composed of subsystems A and B and that an experimenter can interact with each part. If the system is in a pure product state, any local measurements performed on subsystems A and B is associated to statistically independent outcomes, i.e., a probability distribution that factorizes. In fact, such a product state can be prepared by two independent experimenters by means of *Local Operation and Classical Communication* (LOCC), see Fig. 2.2. This is not true for pure non-product states: they can not be prepared locally and will show some degree of correlation in the measurement outcomes.

In the more complex case of mixed states, the concept of *separability* is introduced to distinguish states that exhibit classical and quantum correlations. The state of a bipartite system is defined *classically correlated* or *separable* [24] if it is a convex combination of product states, i. e., if it can be written in the form

$$\rho = \sum_{i=1}^{n} p_i \rho_A^{(i)} \otimes \rho_B^{(i)} \,, \tag{2.20}$$

where $0 \leq p_1, ..., p_n \leq 1$ and $\sum_{i=1}^{n} p_i = 1$. The states $\rho_A^{(i)}, i = 1, ..., n$ are elements of $\mathcal{S}(\mathcal{H}_\mathcal{A})$, while $\rho_B^{(i)} \in \mathcal{S}(\mathcal{H}_\mathcal{B})$. The experimenters can prepare a state in the form of Eq. 2.20 with LOCC by locally producing one of the product states $\rho_A^{(i)} \otimes \rho_B^{(i)}$ with probability p_i and then neglecting the information about which one of the labelled states has been generated. All the states than can not be cast in the form of Eq. 2.20 are defined *entangled*.

While finding a decomposition as in Eq. 2.20 (that is, judging if a state is separable or not) may be easy for low-dimension quantum systems, it is a highly non-trivial problem in the general case. Included in the set of separable states we find another important convex subset of $\mathcal{S}(\mathcal{H})$, the set $\mathcal{P}(\mathcal{H})$ of *Positive-Partial-Transpose* (PPT) states. The *partial transposition* with respect to system B is the transposition operation in $\mathcal{H}_\mathcal{B}$. In the matrix

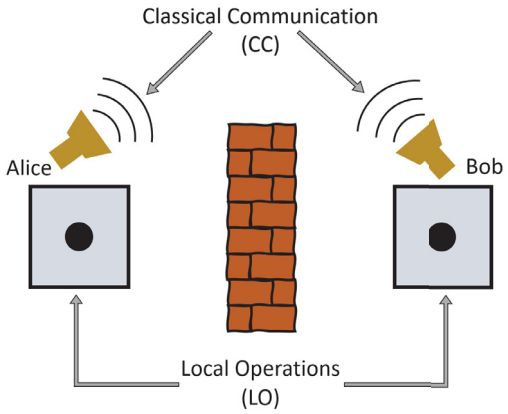

Figure 2.2: Schematic representation of local operation and classical communication.

representation of a state in some orthonormal product basis, if $\rho_{m\mu,n\nu}$ is a generic matrix element, then the partial transpose of ρ with respect to B is

$$\rho^{T_B}_{m\mu,n\nu} = \rho_{m\nu,n\mu} \, . \tag{2.21}$$

Since the transposition operation is not a completely positive map, the partial transposition does not necessarily map states into states, since ρ^{T_B} is not always positive. However, ρ^{T_B} is positive if and only if ρ^{T_A} is positive. A state ρ is then called a PPT state if $\rho^{T_A} \geq 0$. Crucially, it holds for all states ρ

$$\rho \text{ is separable } \implies \rho^{T_A} \geq 0 \, . \tag{2.22}$$

The converse has been proven [25] only for the case of bipartite quantum systems of dimension 2×2 and 2×3, in which case

$$\rho \text{ is separable } \iff \rho^{T_A} \geq 0 \, . \tag{2.23}$$

2.3.1 The Bell states

The Bell states are four maximally entangled quantum states of two qubits that find enormous use in quantum information theory and also in this thesis (Chap. 6 and Chap. 7 for example). Bipartite maximally entangled states have the property that, when partial trace over one of the subspaces is applied, the reduced density operator is proportional to the identity matrix. They can be expressed as follows, where the subscripts 1 and 2 indicate the two qubits

$$\begin{aligned} |\Phi^{\pm}\rangle &= \frac{1}{\sqrt{2}}\big(\,|0\rangle_1 \otimes |0\rangle_2 \pm |1\rangle_1 \otimes |1\rangle_2\,\big) \\ |\Psi^{\pm}\rangle &= \frac{1}{\sqrt{2}}\big(\,|0\rangle_1 \otimes |1\rangle_2 \pm |1\rangle_1 \otimes |0\rangle_2\,\big)\,. \end{aligned} \tag{2.24}$$

They form a maximally entangled basis, known as the Bell basis, of the four-dimensional Hilbert space for two qubits. In Chap. 6 and Chap. 7, when we refer to *Bell state measurement*, we refer to a projective measurement in this basis. A generalization of the Bell states to more than 2 qubits is represented by the *Greenberger–Horne–Zeilinger* (GHZ) states

$$|GHZ\rangle = \frac{|0\rangle_1 \otimes \cdots \otimes |0\rangle_N + |1\rangle_1 \otimes \cdots \otimes |1\rangle_N}{\sqrt{2}}\,, \tag{2.25}$$

where N is the number of entangled qubits.

Cryptography and Quantum Key Distribution 3

Cryptography, the art of creating and breaking codes, played a fundamental role in the history of mankind. From the ancient civilizations to modern warfare, the ability to communicate safely with allies and to crack enemy encoded communications has always been pivotal. The importance of cryptography outside of the military world increased exponentially with the introduction of the internet. Every single piece of information exchanged on the internet is, in principle, publicly available to anyone. Security and confidentiality are obtained through encryption of the plain text and successive decryption by the authorized party, recipient of the communication. Particular attention must be paid when really sensible data are transmitted, like bank transaction authorizations, medical information or military and governmental communications.

The Holy Grail of cryptography is to develop an absolutely secure coding scheme which is secure against eavesdroppers with unlimited power. This goal has been achieved, at least in prin-

ciple, by Gilbert Vernam with the invention of the *One-Time Pad* (OTP) encryption in 1917 [26]. Like in many other modern cryptographic systems, a secure key is employed in the OTP during the encryption and decryption processes. While the encryption and decryption algorithms themselves are publicly known, the security of the cryptographic scheme is guaranteed as long as the key used is secure. A generic symmetric encryption cryptographic protocol, like the one-time-pad, is represented in Fig. 3.1.

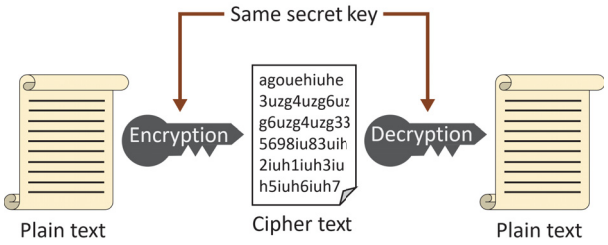

Figure 3.1: Schematic representation of a symmetric encryption cryptographic protocol, like the one-time-pad described in the main text.

OTP is an encryption scheme in which the binary plaintext is encoded by summing it (modulo 2) to a binary key which has the same length at the text itself. The same key is also used by the legitimate receiver, which performs again the sum modulo 2 to obtain the plaintext back. With the assumption that the key is used only once, the absolute security of OTP can be proven [27]. However, once Alice (A, the sender) and Bob (B, the receiver) have used up their pre-shared secure key, the secure communication will be interrupted. The key distribution problem typically involves two tasks which are unachievable in classical physics: truly random number generation and unconditionally secure key distribution through an insecure channel (such as the internet). The first task is made impossible by the deterministic nature of classical physics, true also for chaotic processes. In contrast, true ran-

dom numbers can be generated from elementary quantum processes. The second task,instead, is prevented by the fact that, in classical physics, information can be copied and duplicated. Alice and Bob have no way to prove that a key established through an insecure channel has not been copied by an eavesdropper (Eve or E in the remainder). Otherwise, Alice and Bob could use the same scheme to send secure messages directly.

In most modern cryptographic systems, such as *Advanced Encryption Standard* (AES), much shorter keys are used to encrypt long messages, giving up the provable unconditional security of OTP. This does not fully solve the distribution problem, though.

To circumvent the key distribution problem, public-key cryptographic protocols have been proposed, like the famous *Rivest-Shamir-Adleman* (RSA) scheme. The security of the internet is nowadays based on solutions similar to such a clever and effective idea. Unfortunately, the security of these schemes rests upon unproven mathematical assumptions. For example, the security of RSA is established on the assumption that there is (classically) no efficient way to find the prime factors of a very large integer, which is still unproven despite the effort of generations of mathematicians. Moreover, in quantum computation an efficient algorithm for factorization already exists [9]. So, the entire global communication system could instantly collapse as soon as the first large-scale quantum computer will become available. Even though this moment might still be decades away, this threat is already in action. Eve can store public communications today and decode them when quantum computers will be powerful enough. This is a sizeable problem for information that needs long-term security, such as military communications and health records.

Quantum key distribution, which is the topic of the remainder of the chapter, is a possible and effective solution to this problem. Based on the fundamental principles of quantum mechanics, QKD provides an unconditionally secure method to distribute random keys through insecure channels.

We will start introducing some principles useful to under-

stand where the security of quantum key distribution comes from. Then, the fundamental stages of a QKD protocol are discussed, using the famous BB-84 protocol as an example (Sec. 3.1). The problem of proving security in the non-asymptotic case is briefly addressed in Sec. 3.2. We then analyse the use of weak laser pulses to substitute single photons and how one can take into account this modification in the security proofs in Sec.3.3. (Measurement-)device-independent QKD and multipartite QKD are briefly introduced in Sec. 3.4. Finally, a short review of recent experimental results about QKD in fibre is reported in Sec.3.5.

3.1 Basic principles and the BB-84 protocol

Several inherently quantum principles can be invoked to naively give foundation to the security of different forms of quantum key distribution, e.g., the *no-cloning theorem* [11], the *uncertainty principle* through the *entropic uncertainty relations* [28] or the *monogamy of entanglement* [29]. In the following we will focus on the first one, proving the no-cloning theorem and showing how it can be exploited to secure quantum communications.

3.1.1 The no-cloning theorem

Assume two quantum systems ρ_A and ρ_B associated to the same Hilbert space $\mathcal{H} = \mathcal{H}_\mathcal{A} = \mathcal{H}_\mathcal{B}$. The task is to find a procedure to perfectly copy the state $|\phi\rangle_A$ or ρ_A into the system ρ_B irrespectively of the original state $|\phi\rangle_A$ [11]. We start with the composite system in the product state

$$|\phi\rangle_A \otimes |e\rangle_B \ , \tag{3.1}$$

where $|e\rangle_B$ is some unknown initial state of ρ_B independent of $|\phi\rangle_A$. The target is the following product state

$$|\phi\rangle_A \otimes |\phi\rangle_B \ , \tag{3.2}$$

that we want to obtain applying a unitary operation. The theorem states the following. There is no unitary operator U on $\mathcal{H}\otimes\mathcal{H}$ such that for all normalised states $|\phi\rangle_A, |e\rangle_B \in \mathcal{S}(\mathcal{H})$ (we will omit the $\otimes$ in the following)

$$U\big(|\phi\rangle_A |e\rangle_B\big) = e^{i\alpha(\phi,e)} |\phi\rangle_A |\phi\rangle_B \ , \tag{3.3}$$

where α is real and dependent on $|\phi\rangle$ and $|e\rangle$.

To prove the theorem, an arbitrary pair of states $|\phi\rangle_A$ and $|\psi\rangle_A$ in $\mathcal{S}(\mathcal{H})$ is considered. This chain of equalities holds, due to the unitarity of U

$$\begin{aligned}
\langle\phi|\psi\rangle\langle e|e\rangle &\equiv \langle\phi|_A \langle e|_B |\psi\rangle_A |e\rangle_B && (3.4)\\
&= \langle\phi|_A \langle e|_B U^\dagger U |\psi\rangle_A |e\rangle_B && (3.5)\\
&= e^{-i(\alpha(\phi,e)-\alpha(\psi,e))} \langle\phi|_A \langle\phi|_B |\psi\rangle_A |\psi\rangle_B && (3.6)\\
&= e^{-i(\alpha(\phi,e)-\alpha(\psi,e))} \langle\phi|\psi\rangle^2 \ . && (3.7)
\end{aligned}$$

The quantum state $|e\rangle$ is assumed to be normalized, so we get

$$|\langle\phi|\psi\rangle|^2 = |\langle\phi|\psi\rangle| \ . \tag{3.8}$$

This implies either $|\langle\phi|\psi\rangle^2| = 1$ or $|\langle\phi|\psi\rangle^2| = 0$. Invoking the Cauchy-Schwarz inequality, we have that either $|\phi\rangle = e^{i\beta}|\psi\rangle$ or $|\phi\rangle$ is orthogonal to $|\psi\rangle$. This is clearly in contrast with the assumption of having two *arbitrary* states. Therefore, a single universal unitary U cannot perfectly clone a general quantum state. The assumptions of pure states and unitary operations cause no loss of generality. The result can be extended to mixed states and generalized quantum operations by means of *purification* of the state and the Stinespring dilation theorem (see Eq. 2.17).

3.1.2 Introduction to the BB-84 protocol

The impossibility of making perfect copies of unknown quantum states is indeed a shortcoming in some situations. However, it

can also be harnessed to achieve unconditionally secure key distribution: any attempt by the eavesdropper to learn information encoded in quantum states will disturb them and expose her existence.

In 1984, Charles H. Bennet and Gilles Brassard, extending previous ideas by Stephen Wiesner, published the first complete quantum cryptographic protocol, denominated BB-84 [10]. The setup is very simple: two parties, Alice and Bob, are inside secure laboratories and are connected by an insecure quantum channel and an authenticated classical channel. The eavesdropper Eve has full control over the quantum channel and can listen to, but not interfere with, the classical channel. Alice sends qubits, encoded in the polarization degree of freedom of photons, to Bob through the quantum channel. She selects two mutually unbiased bases, for example the computational basis $\{|0\rangle, |1\rangle\}$ and the diagonal basis $\{|+\rangle, |-\rangle\}$, where $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. The states $|0\rangle$ and $|+\rangle$ will be associated with the bit 0 while $|1\rangle$ and $|-\rangle$ with 1. At every round of the protocol, Alice chooses at random the bit to send and the encoding basis. A pictorial representation of the scheme is shown in Fig. 3.2. Without knowledge of Alice's basis selection, Bob randomly chooses either computational or diagonal basis for each incoming photon and register the outcome. If Alice and Bob happen to use the same basis, their results are perfectly correlated, while they are uncorrelated otherwise. In the next stage, called *sifting*, Alice broadcasts her basis selection and they discard all the instances in which they prepared/measured in different bases, that led to uncorrelated results. In the absence of environmental noise, system imperfections and Eve's disturbance, their sifted keys are identical.

The availability of the authenticated classical channel is essential to avoid possible *man in the middle* attacks, in which Eve impersonates the other party. The authentication can be assured if Alice and Bob share a short secure key in advance. This makes a QKD protocol, more appropriately, a key expansion protocol.

Eve can launch a simple *intercept-resend* attack: she intercepts

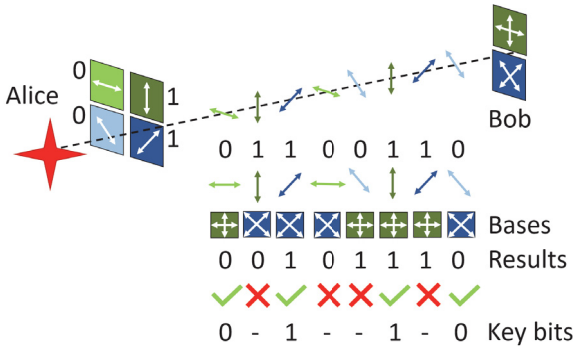

FIGURE 3.2: Scheme of the BB-84 cryptographic protocol, with bit and basis selection, measurement result and sifting.

the photons sent by Alice, she performs (like Bob) a measurement in one of the two bases at random and resends a new photon to Bob according to her measurement result. In the cases that survive sifting, if Eve happens to use the correct basis, then both she and Bob will decode Alice's bit correctly (she leaves no trace). On the other hand, when she uses the wrong basis, both she and Bob will have a measurement result uncorrelated with Alice's bit. The legitimate parties now compare a subset of the sifted key on the public channel. This procedure is the so-called *parameter estimation stage* and it allows them to estimate the *Quantum Bit Error Rate* (QBER) of the key distribution run. This parameter is linked to the perturbation introduced by Eve in the quantum channel and so, consequently, to the amount of information that she extracted about Alice's key. In the case of the intercept-resend attack, a QBER of at least 25% is expected on average, so Eve's presence can be easily detected. More general attacks can be performed by Eve and can be taken into account in the security proofs. However, the basic principle behind the security of QKD remains valid, namely, that Eve will always introduce disturbance in the quantum states when she tries to gain information about

the key.

Errors in the sifted keys, however, will also originate from intrinsic noise sources of the QKD system, so even in the absence of an eavesdropper. Error correction techniques are applied during the *information reconciliation* stage, to establish a perfectly correlated key between Alice and Bob. In doing so, they will leak some information about the key to Eve. She will, in the end, have partial information about the key, coming from her attack during the exchange of quantum states and from the error correction leakage. The parameter estimation is fundamental in this case, since it allows Alice and Bob to estimate the amount of information gained by Eve. In the event that Eve has too much information, no secure key can be generated, the protocol must abort and Alice and Bob start over again. If the information leaked is below a certain threshold, instead, the legitimate parties can perform *privacy amplification* algorithms to generate a new secure key. The total length of the key will be shortened but the information that Eve has about it will be exponentially small.

For a protocol like BB-84 the secure key-rate, defined as the ratio between the generated key length and the length of the raw key, can be expressed as follows, under the assumption of collective attacks in the asymptotic case (see [30] for details)

$$r = \lim_{m\to\infty} \frac{m'}{m} = H(X|E) - H(X|Y)\ . \qquad (3.9)$$

Here $H(.|.)$ is the conditional von Neumann entropy. The registers X and Y refer to the Alice's and Bob's keys respectively and E represents Eve's information. Very intuitively, the expression states that the secure key rate is equal to the uncertainty that Eve has about the raw key bits X, minus Bob's uncertainty.

The protocol above was pictured in the so-called *prepare and measure* view. The equivalent protocol can be described in the *entanglement-based* picture in the following way. At every round, Alice prepares a bipartite system in a specific entangled state and sends one half of it to Bob. The parties then measure their half of

the state, obtaining correlated or uncorrelated results depending on the state and basis choice, just like in the prepare and measure picture. This alternative point of view, although generically more complicated to reproduce experimentally, is often assumed in security analysis since it can make it easier to deduce general results.

3.2 Finite-key effects

A common weakness of many security proofs in the first years of QKD is the asymptotic resource assumption. It corresponds to assuming that an arbitrarily large number M of signals is exchanged between Alice and Bob and utilized to compute the final key rate. Practical realizations cannot meet this requirement, in fact, keys are usually computed from a relatively small number of signals ($M < 10^6$). Modern security proofs generally take into account this aspect and try to obtain bounds on the key rate as tight as possible, to minimize the minimum number of signals necessary to obtain a secure key.

In addressing this problem, the first step is to give a proper definition of *security* of a QKD protocol, which stays valid in the non-asymptotic regime. Most generally, the security of a key K can be expressed as its deviation ϵ from a perfect key. The latter can be defined as a uniformly distributed string of bits which is completely independent of the eavesdropper's knowledge. In the asymptotic scenario, a key K of length m is usually defined secure if the deviation ϵ tends to 0 when m increases. In the non-asymptotic regime, however, the deviation remains always finite, so an operational interpretation to it must be found. It is then possible to attribute a physically meaningful value to the security threshold ϵ. A second very relevant aspect is the composability of the security definition. This condition ensures that the QKD protocol can be securely composed with other communication applications. In other words, the key generated by a QKD protocol

can safely be used, for example as a one-time-pad for encryption. This requirement is clearly fundamental for any practical use of QKD.

A standard definition of security that meets both requirements, namely, it is composable and the parameter ϵ has an operational interpretation, is the following [31]: for any $\epsilon \geq 0$, a key K is defined ϵ-secure if the state ρ_{KE} satisfies this condition

$$\frac{1}{2}||\rho_{KE} - \tau_K \otimes \rho_E||_1 \leq \epsilon \, . \tag{3.10}$$

Here ρ_{KE} is the joint classical-quantum state of the key K and the quantum system hold by E. τ_K is the completely mixed state on K and ρ_E is the reduced state of E's system. This definition says that parameters ϵ is the maximum probability that the key K differs from a perfect key (a fully random bit string uncorrelated with the adversary). Equivalently, ϵ can be considered as the maximum failure probability, where a failure corresponds to the case when the adversary might have gained information about K. The failure probability of any cryptosystem with a perfect key only increases by at most ϵ when it is replaced by an ϵ-secure key [31], ensuring composability of the security definition. As an example, it follows that OTP encryption with an ϵ-secure key fails to be confidential with probability at most ϵ, since the OTP scheme has failure probability 0 with a perfect key. Important differences between the asymptotic and non-asymptotic case are in the parameter estimation stage. After exchanging M signals, the parties publicly reveal a random sample consisting of n of the pairs of values obtained by Alice and Bob measuring the states. Both parties now hold a string of length $m = M - n$. For many schemes, the ratio n/M can be chosen arbitrarily small for sufficiently large M. In other words, an infinitesimally small fraction of the signals is sufficient to accurately estimate the parameters of the channel, when M goes to infinity. The above considerations are clearly no longer valid in the non-asymptotic scenario, when M is finite. One has to optimize the trade-off between the length

of the raw key m and the precision of the parameter estimation. Similar considerations apply to the sifting stage, even for biased basis choice one has to subtract the discarded signals from the final key length. Another deviation from the asymptotic case can be found in the performance of the error correction procedure, which is generally lower in non-asymptotic case. Finally, the last aspect is that, as already mentioned, the security of a key generated in the non-asymptotic scenario is always finite and the final length of the secure key depends on the chosen security parameter ϵ.

An important ingredient in the evaluation of the key rate in the non-asymptotic scenario is the so-called smooth min-entropy $H_{\min}^{\epsilon}(A|B)$, a generalization of the von Neumann entropy (used in Eq. 3.9). For any bipartite state ρ_{AB} and $\epsilon \geq 0$, the smooth min-entropy $H_{\min}^{\epsilon}(A|B)$ is defined as the maximum, taken over all the states $\bar{\rho}_{AB}$ in an ϵ-ball around ρ_{AB}, of the following quantity

$$H_{\min}(A|B) := -\log_2\left(\min\left\{\lambda > 0 : \exists \sigma_B : \bar{\rho}_{AB} \leq \lambda \mathrm{id}_A \otimes \sigma_B\right\}\right). \tag{3.11}$$

Here id_A indicates the identity operator on system A and σ_B is a generic density operator on system B. The smooth min-entropy specifies the number of uniform bits that can be extracted during the privacy amplification stage.

Without going into the details of the protocol and the assumptions (more can found e.g. in [31]) the length of an ϵ-secure key can be bound by an expression of this form

$$m' \leq H_{\min}^{\bar{\epsilon}}(X^m|E^m) - \mathrm{leak}_{EC} - 2\log_2\left(\frac{1}{2(\epsilon - \bar{\epsilon} - \epsilon_{EC})}\right). \tag{3.12}$$

Here X^n is the register of Alice's key and E^n is Eve's overall quantum state. leak_{EC} is the number of bits leaked during

the error correction, $\bar{\epsilon} \geq 0$ and $\epsilon_{EC} \geq 0$ is the security parameter connected to the error correction procedure. The problem is now the computation of the min-entropy, depending on the class of attacks allowed to Eve and the protocol, details can be found for example in [31, 32]. The imprecision in the parameter estimation, inherent to the non-asymptotic scenario, needs to be suitably handled in computing the min-entropy.

3.3 Weak coherent pulses and the decoy-state method

Deterministic sources of single photons are still in their first stages of development. So, alternative solutions have been devised, e.g., probabilistic sources of single photons and *Weak Coherent Pulses* (WCP). The latter consist in highly attenuated laser pulses. This substitution, however, has to be taken into account when analysing the security of the QKD protocol, to avoid the creation of loopholes that the adversary can exploit. A heavily attenuated laser pulse can be identified with a coherent state with a small average photon number. Coherent states consist in a superposition of different photon number states. No matter how small the average is, there is always a non-zero probability that the laser pulse contains more than one photon. In this case, the eavesdropper can exploit the very powerful *Photon Number Splitting* (PNS) attack [33]. In this attack, Eve performs a *Quantum Non-Demolition* (QND) measurement to learn how many photons Alice's laser pulse contains without disturbing the encoded quantum information. If it consists of only one photon, the signal is blocked and Bob will not receive anything. If the laser pulse contains more than one photon, instead, Eve keeps one photon for herself and sends the rest to Bob through a lossless channel. Eve stores the intercepted photons in quantum memories (discussed later in Chap.6) until Bob announces his measurement bases. Then she measures the stored photons in the same basis as Bob. In the end, Eve has

exactly the same outcomes as Bob, so no secure key can be generated. Only the single-photon pulses can be considered secure, while all the multi-photon pulses are completely insecure. One can choose a very small average photon number to suppress the multi-photon probability, increasing at the same time the probability of sending a vacuum state, which in turn lowers the efficiency of the communication. The final result is that the secure key rate scales quadratically with the transmittance of the channel, while it scales linearly with a true single photon source.

A fundamental breakthrough corresponded with the introduction of the decoy state method [34]. The PNS attack is based on the idea that the eavesdropper can recognise single-photon pulses and block them. As a result, the quantum channel between Alice and Bob (thus including the action of Eve) have a transmittance that depends on the photon number of the signal, so it is not a passive channel. Testing the quantum channel during the QKD session, the PNS attack can be detected and the protocol can be aborted. In decoy-state QKD, the unknown channel is tested analysing its response to different input signals. Alice and Bob perform the standard QKD operations with weak laser pulses with different photon numbers, generally one "signal state" and one or more "decoy states", and evaluate separately the transmittance and QBER for every intensity. If Eve performs the PNS attack, she will inevitably introduce a different amount of losses for signal and decoy states, that can be detected. It can be proven that the linear scaling with the transmittance can be recovered with the decoy state method. The first security proofs relied on an infinite number of decoy states. It has been shown soon later that the much simpler vacuum+weak decoy state method achieves a key rate very close to the infinite decoy state case [35]. A crucial assumption in the decoy-state protocols is that the signal state and decoy states are identical except for their average photon numbers. In this way we ensure that Eve has no way of telling whether what she receives originated from the signal state or the decoy states. If this assumption is not verified with good precision by the prac-

tical implementation, the corresponding loophole can be easily exploited by Eve, breaking the security.

A complete analysis of the security of the asymmetric BB-84 protocol with WCPs and taking into account finite-key effects can be found in [36], which is also used for the results reported in [17] and Chap. 9.

3.4 More Quantum Key Distribution schemes

After the success of the BB-84 protocol, especially using WCPs and the decoy-state method, a plethora of QKD protocols have been proposed in the literature. We are going to discuss now, very briefly, different families of QKD protocols, that either relax some of the assumptions to prove security or achieve more general results.

The BB-84 protocol previously discussed is one of the so-called device-dependent QKD protocols. The security claims totally rely on the assumption that the parties and their devices, like sources, polarization analysers and detectors, are protected by the action and control of the eavesdropper. In other words, they are contained in secure labs that communicate with each other (and the eavesdropper) only through the authenticated classical channel and the insecure quantum channel. An additional important assumption is that these devices are characterized, e.g., Bob's measuring apparatus actually measures in different basis when he decides to do so. These assumptions can be very complicated or even impossible to ensure in a practical implementation. That is why a huge theoretical and experimental effort has been put into devising new protocols whose security can be proven with relaxed assumptions.

The receiver's side of the QKD protocol, state analyser and detectors, constitute generally the weaker link of the chain. The eavesdropper can exploit several quite common imperfections to obtain side-channel information and break the security of the pro-

tocol. This is the reason why *Measurement Device Independent Quantum Key Distribution* (MDI-QKD) has been developed. In this family of protocols, both Alice and Bob are equipped with QKD transmitters and send their signals to a middle node, generally called Charlie. In the security analysis, the control of the middle node is given to the eavesdropper, so all the assumptions about the QKD receiver are relaxed. The central node performs a joint measurement on the signals sent by the two parties, projecting the joint state in the Bell basis. The measurement performed in the central node, when done in the legitimate way, will highlight correlations between the signals sent by Alice and Bob, that can be used to extract a secure shared key. The full security proof can be found, for example, in [37].

A family of measurement-device-independent protocols that has been recently proposed and received enormous attention is the so-called *Twin-Field Quantum Key Distribution* (TF-QKD) [38, 39]. This new approach allows to achieve a key rate that scales as the squared root of the transmittance of the link. This result is possible thanks to a different way of encoding and retrieving the information in the quantum carriers used for the protocol. In TF-QKD the information is encoded in the phase of the optical pulses prepared by the two users that want to establish the secure communication, and the secret key is retrieved via a single photon interference measurement made by the middle node. Theoretical [38] and experimental [39] works proved that these protocols are able to overcome the so-called *Pirandola-Laurenza-Ottaviani-Banchi* (PLOB) bound, the maximum key rate that is achievable over a certain channel loss without the use of repeaters.

The pinnacle of cryptography in terms of the number of assumptions is represented by *Device Independent Quantum Key Distribution* (DI-QKD). In this case the devices used need not be characterised, apart from a source of local randomness per party. Alice and Bob only need to verify that the input-output statistics of the devices they own violate some Bell-like inequality [40], like the *Clauser-Horne-Shimony-Holt* (CHSH) inequality [41]. The

entangled states measured by such devices can even be provided by Eve herself. A malicious attempt by the eavesdropper can be detected by analysing the input-output statistics and an information-theoretically secure key can be extracted [42].

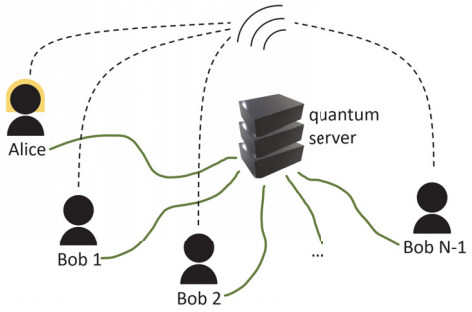

Figure 3.3: Schematic representation of a multipartite QKD scheme, in which the multipartite entangled state is sent by a central quantum server to the legitimate parties through quantum links (dark green lines). The classical channels are pictured as black dashed lines.

When a multipartite entangled state is available, multipartite quantum key distribution can be performed, see Fig. 3.3. A big fraction of today's communication systems are not based on point-to-point links but on complex networks. In the advent of quantum technologies, much effort is devoted to building quantum networks and creating global quantum states across them. Thus, the generalisation of quantum key distribution to multipartite scenarios is topical. In order to establish a common secret key (the conference key) among N parties, one can follow two main paths: building up the multipartite key from bipartite QKD links, or exploiting correlations of genuinely multipartite entangled states. Truly multipartite QKD has been proven to be advantageous in several situations, for example in networks with bottlenecks [43]. This concept has also been extended to MDI- and TF-QKD [44].

3.5 State of the art experimental results in fibre

In the fast-growing field of QKD, advancements in security proofs and design of new protocols went and is going hand in hand with better and better experimental realizations. In this subsection we are going to list some of the recent experiments and field applications that pushed forward the limit of what QKD can achieve.

In 2018, the record distance for prepare and measure QKD has been set to 421 km. The authors utilised *Superconducting Nanowire Single-Photon Detectors* (SNSPDs) with an extremely low number of dark counts and ultralow-loss fibres. Using these components combined with a modification of a loss-tolerant protocol with three-state time-bin encoding and a one-decoy approach, the team achieved the best long-distance performance to date for fibre-optic QKD. For lengths of fibres ranging from 251 to 404 km, the scheme achieved key rates that were over 100 times higher than previous demonstrations over the same distances, and they remained positive up to a record distance of 421 km. The increase in the key rate was provided by a QKD setup developed recently by the same authors, featuring one of the highest repetition rates (2.5 GHz) ever used in QKD experiments. The researchers also proved the stability of the system by running it for more than 24 hours.

Before this result, the record distance belonged to an implementation of MDI-QKD. Using a WCP-based MDI-QKD protocol with the 4-intensity decoy method, the authors achieved non-zero key rate at a distance of 404km of ultralow-loss fibre [45]. This result was achieved with a much slower source repetition rate as the one reported above, 75 MHz, due to the higher complexity of the detection scheme.

The MDI-QKD got the record back with several implementations of TF-QKD in the last 2 years. A very recent result [46] reported a record distance of 511km of ultralow-loss fibre, amounting to over 89dB of loss. To make this result even more valuable, it was obtained over a deployed long-haul fibre link, between the

cities of Qingdao (Alice), Jinan (Bob) and Mazhan (Charlie) in China. The secure key rate obtained is around 3 orders of magnitudes greater than what is expected if the previous QKD field test system over the same length were applied. The efficient quantum-state transmission and stable single-photon interference over such a long distance in a deployed fibre paves the way towards large-scale fibre quantum networks.

Satellite-based Quantum Key Distribution 4

Despite the enormous advancements of the last years [39, 47], scaling the maximum distance of quantum communication beyond few hundred km is extremely challenging. The exponential losses experienced by the light sent through optical fibres (the standard channel used in classical modern communication) becomes too hindering beyond that threshold. Quantum repeaters [18, 48] might be the solution in the future, once the technical difficulties involved are surpassed. Optical links between satellites and ground stations (an example is pictured in Fig. 4.1) can, on the other hand, achieve quantum communication at lengths over 1000km [12, 13]. Free-space optical links consist of two main components. The transmitter telescope sends a light beam towards the receiving station. The receiver telescope collects the light which is then properly analysed.

The advantage of satellite-based links resides in the quadratic scaling of the transmittance with the distance inherent to free-space optical links in vacuum. The losses are due to diffraction

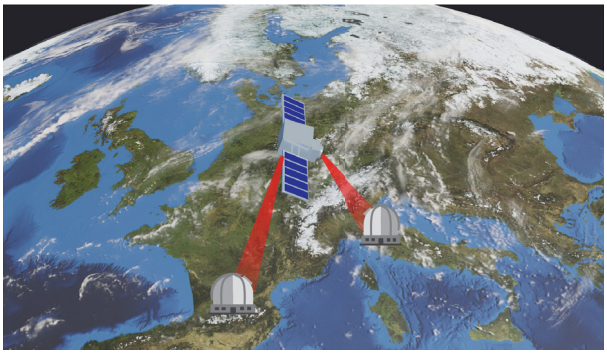

Figure 4.1: Pictorial representation of a double downlink between a low Earth orbit satellite and two ground stations on the ground.

of the propagating optical beam and the finiteness of the receiving area. Such advantageous scaling is generally lost for propagation in the atmosphere, as described in more detail in Sec. 4.2. The simplest satellite-based configurations are given by downlinks and uplinks. The former consist in satellite-to-ground links, in which the transmitter is onboard the satellite and the receiver is in an optical ground station. In the latter, instead, the ground station sends the light towards the satellite, where the receiver is placed. Downlinks exhibit much higher transmittance then uplinks at fixed parameters, as better discussed in Sec. 4.3. The reason is that in downlinks the atmospheric effects happen only at the end of the propagation, introducing a small amount of losses. In uplinks the additional beam broadening that happens at the beginning of the propagation greatly enlarges the total losses.

Several feasibility studies have analysed the different aspects of the implementation and tried to find the best use cases. In [49] the authors estimate the expected losses and noise coming from environmental light and compute the key rate for different QKD protocols. In [50] a comprehensive design and performance analysis of *Low Earth Orbit* (LEO) satellite quantum communication

is performed. Optimal telescopes sizes and wavelength of the quantum signals are studied and the possibility to perform long-distance Bell tests and quantum teleportation is evaluated. A review of recent progress in satellite quantum key distribution can be found in [51], concerning experimental results and proposals.

In the remainder of this chapter we will, first of all, review some of the recent experimental results in the field of satellite-based quantum communication (Sec. 4.1). Afterwards, we focus on the theoretical problem of modelling the properties of a free-space optical link, in Sec. 4.2. Finally, we apply this analysis to the case of satellite-based links and we review some of the results of our recent publication [17] in Sec. 4.3, concerning satellite quantum links with different weather conditions.

4.1 State of the art experimental satellite quantum communication and proposals

In the past twenty years there have been significant efforts to develop the basic technologies required for QKD in space. Quantum communication has been accomplished over a 144km-long terrestrial free-space link at the Canary islands [52]. Demonstrations with moving terminals have been performed to emulate the motion of a satellite [53]. Experiments using passive corner-retroreflector satellites proved for the first time the ability to detect single photons coming from orbiting spacecrafts [54]. Using the Japanese micro-satellite SOCRATES, with a mass of just 48 kg, scientists were able to achieve quantum-limited communication in a LEO-to-ground link [55]. The real revolution in the field was attained with the Chinese research project *Quantum Experiments at Space Scale* (QUESS) and the mini-satellite Micius, operated by the Chinese Academy of Science. The results obtained had a substantial impact not only in the academic world, but also in industry and public opinion.

The satellite, with a total mass of 640 kg, has been launched

on August 15, 2016, on a Long March 2D vehicle from Jiuquan Satellite Launch Center in the Gobi desert, Inner Mongolia. It travels on a Sun-synchronous orbit with an average altitude of 500 km. It transports two Cassegrain telescopes of 30cm and 18cm diameter aperture. It is fitted, along with several other service payloads, with a high-bandwidth and high-precision multi-stage *Acquiring, Pointing and Tracking* (APT) system. It allowed, in conjunction with similar systems on the ground, to establish optical links with several ground stations both inside China (Xinglong, Nanshan, Delingha...) and outside (Graz). The diverse array of scientific payloads onboard allowed the achievement of several groundbreaking experimental results. Using a decoy-state QKD transmitter at a wavelength of 850nm with polarization encoding, satellite-to-ground QKD has been achieved with kHz key rate over a distance of up to 1200 km [12]. A source of entangled photons at 810nm based on *Spontaneous Parametric Down-Conversion* (SPDC) allowed to distribute entanglement between two ground stations separated by 1200 km with a fidelity $F \sim 0.87$ [15]. The photons have been used to obtain a violation of a CHSH-type Bell inequality by four standard deviations, without the locality and freedom-of-choice loopholes. The same payload was also used to implement an entanglement-based QKD protocol [13]. Ground-to-satellite quantum teleportation has been executed using the on-board polarization analyser, with fidelity well above the classical limit [14].

In the following we will give some details about one of the last experimental runs involving Micius [56]. The authors report the results of an integrated hybrid quantum network based on trusted nodes. It is composed by the 2000km-long Beijing-Shanghai quantum communication network [57], local networks in Beijing, Jinan, Hefei and Shanghai and, finally, the satellite link connecting Nanshan and Xinglong (the latter linked to Beijing).

The results considering the entirety of the hybrid quantum network can be found in [56]. Here we focus on the performance

of the satellite links, since a significant improvement over the first experimental runs (see [12], for example) has been achieved. We refer in particular to Fig. 3a of [56]. The QBER is kept below 1% for almost the entirety of the overpass, showing that during nighttime the environmental light is absolutely marginal. The sifted key rate goes up to almost 500kbps, a great improvement with respect to what was reported in 2017 in [12] (around 15kbps). The authors specify that improvements were implemented regarding the repetition rate of the source, the optical spatial-mode matching and the spectral filtering.

These groundbreaking results have spurred an international quantum space race. The goals are the establishment of national and international global quantum communication networks and the development and deployment of the architecture to merge different quantum technologies, such as sensing and computing, to build the future quantum internet. Besides China, other countries that are taking part in the race are Japan [55], Canada (QEYSSat) [58], Luxembourg (QUARTZ) [59], United Kingdom (QKDSat, QUARC) [60], Austria/France (NanoBob) [61], Germany (QUBE) [62], Singapore (QKD-Qubesat) [63].

4.1.1 Nano-satellites and CubeSats

Several of the proposals nominated at the end of the previous section assume the use of nano-satellites, which have by definition a mass between 1 and 10kg. This allows an enormous reduction of the cost of the mission, imposing, on the other hand, very strict restriction in terms of power budget and space. CubeSat [64, 65, 66, 67, 68, 69] is a standard platform for nano-satellites that allows to take advantage of a very rich selection of off-the-shelf components for both service and scientific payloads. An additional important cut to the mission cost is related to the launch, since tens of such small spacecrafts can be launched at once. With proper design, CubeSats can be equipped with optical elements with diameter of $\sim$20cm [61], which may allow performance compara-

ble to the much heavier and more expensive Micius.

4.2 Free-space optical links: phenomenology and modelization

A great effort has been put in the last years into the investigation of atmospheric quantum links. Such channels might be extremely handy in some applications. They are mobile, do not require access to the optical fibre infrastructure and can potentially establish global quantum networks via satellites. Some phenomena unknown in the fibre-based implementation, though, can severely limit the efficient performance of quantum protocols over free-space channels. The most important ones are diffraction, turbulence, random scattering and absorption losses in air. The scattering and absorption contributions introduce energy losses and degradation of the signal intensity. Any optical beam also undergoes amplitude and phase modifications due to the random fluctuations of the refractive index in the atmosphere. These random variations are turbulent in nature and are caused by the disordered mixing of air layers with different temperature, pressure and humidity content [70, 71]. Turbulent air motion consists in air eddies and vortices with various sizes, spanning a wide range of scales. This aspect significantly complicates the theoretical investigation of the problem, making a statistical approach practically necessary. During the propagation through the atmosphere the optical beam will undergo random deflections as a whole, usually connected with turbulent eddies of sizes comparable with the width of the beam. When the vortices are much smaller than the beam, instead, the main net effects will be random broadening and deformation of the optical amplitude and phase distribution. These two phenomena are pictured in Fig. 4.2. The aforementioned effects (broadening, deformation and absorption) become even more pronounced if the meteorological conditions depart from what is usually considered clear sky. Additional broaden-

ing, absorption and back-scattering due to random interaction with dust particles, aerosols and precipitations can affect the optical beam.

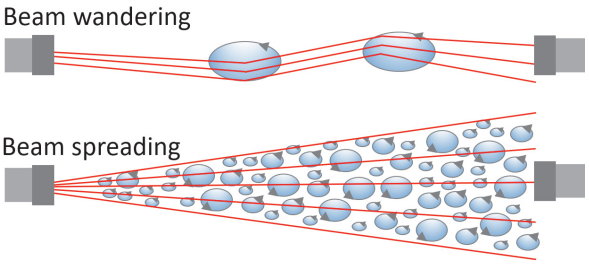

FIGURE 4.2: Pictorial representation of the main effects of turbulence on the propagation of a light beam. Large turbulent eddies induce deflections of the beam as a whole, while smaller ones increase its spreading rate and deform it. The two contributions are present at the same time in the atmosphere.

Several different approaches have been proposed throughout the years to study the propagation of light beams in turbulent atmospheric channels.

In a very popular numerical approach the turbulent medium is represented by a series of independent random phase screens [72, 73, 74]. The split-step technique is used to propagate the beam, generally relying on the parabolic or Fresnel approximation of the wave equation. The screens are generated mainly by using two different techniques. The first is the Fast Fourier Transform-based or spectral method, see for example [75]. The second one is the covariance matrix method, developed in [76], generally more accurate. Nevertheless, the huge amount of computational effort required to evaluate large covariance matrices limits the practical size of the generated screens, thus making necessary the use of fractal interpolation techniques [76].

A different approach can for example be found in [50]. Here the pointing errors and the beam broadening introduced by tur-

bulence are incorporated in the theory by convoluting the corresponding probability distribution with the expected intensity distribution in the Rayleigh-Sommerfeld diffraction theory. This approach, however, is only used to obtain the transmittance of the link when it is averaged over periods of times much longer than the intrinsic variation times of the atmospheric channel (tens of ms).

Many works have been devoted to find the analytical probability distribution that better mimics the experimentally measured transmittance of free-space optical links. Mainly used are the log-normal [77, 78], Gamma-Gamma [79] and Double Weibull [80] distributions. Each of them appears to be more suitable depending on the strength of the turbulence, the length of the link and the configuration of the transmitting and receiving telescopes.

The last approach that we want to present is based on the so-called *elliptic beam approximation* [81] and is at the basis of our recent publication [17], discussed in more detail in Sec. 4.3 and attached to this thesis (Chap. 9). As already said, the light beams will undergo deflection as a whole and broadening when they propagate in a turbulent medium. If we start with a Gaussian beam, in the TEM_{00} mode [82], the simplest form of deformation consists in turning the circular profile of the beam into an ellipse, with the axes suitably rotated. The generic shape of a light beam after the effect of strong turbulence might be very complicated and difficult to describe. In the elliptic beam approximation, instead, this problem is greatly simplified. Five parameters are enough to describe the state of the beam at the receiver: the x and y position of the beam centroid, the two axis of the elliptical profile and the angle of orientation of the ellipse with respect to the coordinate system. In [83] the solution of the paraxial wave equation in the form of phase approximation of the Huygens-Kirchhoff method is written as

$$u(\rho, L) = \int_{\mathbb{R}} d^2\rho' u(\rho', 0) G_0(\rho, \rho'; L, 0) \times \exp[iS(\rho, \rho'; z, z')] \, . \quad (4.1)$$

Here $u(\rho, L)$ is the beam envelope at distance L and position ρ in the transversal plane, $G_0(\rho, \rho'; L, 0)$ is the Gaussian integral kernel describing the propagation in vacuum, while $S(\rho, \rho'; z, z')$ contains all the atmospheric effects. The S term can be written in terms of the relative permittivity $\delta\epsilon$ (or, equivalently, the relative index of refraction). This quantity can be separated into two contributions

$$\delta\epsilon = \delta\epsilon_{\text{turb}} + \delta\epsilon_{\text{scat}} \, , \quad (4.2)$$

corresponding to turbulence and random scatterers, that model dust particles, fog or haze. The statistical properties of these two quantities can be modelled. The authors in [83] show then how to extract the statistical distribution of the values of the parameters of the elliptic beam, based on the theory introduced above. One can then compute the *Probability Distribution of the Transmittance* (PDT), the most important figure of merit for atmospheric links. More details can also be found in [81, 17]

4.3 Satellite-based links for Quantum Key Distribution: beam effects and weather dependence

In this section we review the main ideas and results of our recent publication [17], reported in Chap. 9, in which we model satellite-based links with different weather conditions. The work is based on the theory introduced in the previous section about the elliptic beam model, developed in [81, 83]. We generalize their results (obtained for a uniform link) to the case of satellite-based links, which are non-uniform. Regarding this, it is important to notice

that the computation of the term $S(\rho, \rho'; z, z')$ in Eq. 4.1 involves an integration of the atmospheric effects along the propagation path.

The parameter describing the strength of the turbulence is the so-called refractive index structure constant C_n^2. For the scattering on particles like fog and haze it is n_0, the density of scatterers. They allow to take into account the main contributions describing different weather conditions. These quantities vary as a function of the height in the atmosphere. We assume a simplified model, with a uniform atmosphere up to an effective thickness $\bar{h}$ and vacuum afterwards. This corresponds to the following expressions for down and uplinks

$$\begin{aligned} \text{Downlinks} \qquad & C_n^2(z) = C_n^2\,\Theta(z-(L-h)) \\ & n_0(z) = n_0\,\Theta(z-(L-h)) \\ \text{Uplinks} \qquad & C_n^2(z) = C_n^2\,\Theta(h-z) \\ & n_0(z) = n_0\,\Theta(h-z)\,, \end{aligned} \tag{4.3}$$

where $\Theta(z)$ is the so-called Heaviside step-function, z is the longitudinal coordinate, L is the total length of the link and h is the length travelled inside the atmosphere. To give a sense of scale, consider that the altitude of a low Earth orbit is between 400 and 2000km, while the thickness of the atmosphere is just about $\bar{h} = 20$km. At that altitude the density of the atmosphere is so low that the effects on the propagation of light beams can be considered negligible (more details in Chap. 9).

We then compute the first and second moments of the probability distributions of the elliptic beam parameters at the receiver, as discussed in the appendix of [17]. The PDT can then be estimated through random sampling, obtaining substantially different results for down and uplinks (Fig. 3 and Fig. 4 of Chap. 9). We report in Fig. 5 and Fig. 6 of Chap. 9 the mean transmittance as a function of the angle from zenith between the ground station and the satellite, for downlinks and uplinks. The results

are computed for day- and night-time and for different weather conditions, corresponding to different pairs of values of C_n^2 and n_0. We observe the expected behaviour, with uplinks performing much worse than downlinks (the effect is also pictured in Fig. 4.3). Also, changing weather conditions has a much greater influence on uplinks than on downlinks.

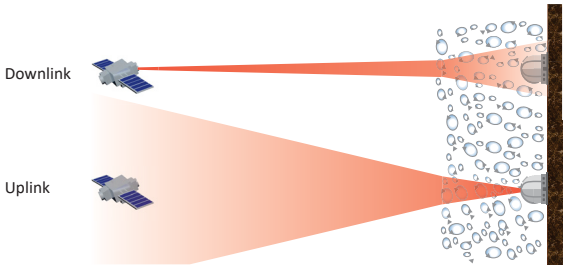

FIGURE 4.3: Depiction of the different effects of the atmosphere on a light beam in the downlink and uplink configurations. In a downlink, the turbulence acts only at the end of the propagation, inducing quite small beam broadening. This effect, on the other hand, happens at the beginning of the propagation for an uplink. The increased angular divergence that it induces makes the performance of an uplink much worse than a downlink, as supported by the results discussed in the text.

The transmittance shown in Fig. 5 and Fig. 6 of Chap. 9 can now be used to compute the expected secret key rates of a QKD protocol. In the following we analyse the performance of the BB-84 protocol [10] with polarization encoding, implemented using either a true *Single Photons* (SP) source or WCP. We use modern techniques to compute the secret key rates for SP [32] and WCP with decoy states [84, 85, 86, 36], taking into account finite-key effects. The key rates are averaged over the PDT computed for different link lengths and configurations. More details can be found in the appendix of [17]. The key rates and the expected QBER are reported in Fig. 7 and Fig. 8 of Chap. 9 as a func-

tion of the angle from zenith between the ground station and the satellite.

The results discussed up to this point assume transmitter and receiver telescopes of 15 and 50cm radius, respectively. This numbers are compatible with the hardware used in the experiments involving Micius (see Sec. 4.1 for details). In Sec. 5 of the paper (Chap. 9) we also analyse the case of smaller satellites, like CubeSats, equipped with much smaller optical elements, confirming the feasibility of long-range quantum communication also in this situation.

4.4 Noise from environmental light

So far in this chapter we have only discussed the problem of estimating the transmittance of an atmospheric optical link. Noise is also extremely important in communication, so the stray light in the different situations needs to be estimated. In a free-space link, environmental photons are usually the most important source of noise. In order to tag the photons and perform a time filtering on the incoming signal, accurate time synchronization between sender and receiver is essential. On top of that, spectral filtering is applied to further reduce the amount of detected noisy photons. The amount of stray light collected also depends generally on the field of view of the receiver telescope. For up-links, during nighttime and for low artificial light pollution, the biggest fraction of environmental photons comes from the Sunlight reflected first by the Moon and then by the Earth [49]. For down-links, the evaluation of the background photons is strongly site-dependent. The power received by the telescope is directly proportional to the parameter H_b, the total brightness of the sky background, that depends on the hour of the day and the weather conditions [87]. These effects have been taken into account in the results discussed in the previous section. More details can be found in the appendix of [17] and Chap. 9.

Realistic Threat Models for Satellite Quantum Key Distribution 5

One of the main strengths of Quantum Cryptography is that the security of the protocols can be proven in an information-theoretic way, for a generic eavesdropping scenario in which the adversary is only limited in its attacks by the laws of quantum physics. This implies that, in some situations, the bounds on the secret key rate that we compute are extremely pessimistic, given what a real eavesdropper can do with today's technology.

Such assumptions are quite difficult to challenge when the quantum communication is performed over optical fibre. In the satellite-based case, instead, as in other free-space optical channels, less pessimistic assumptions might be introduced, without compromising the practical security of the communication. In the satellite-based implementation, for example, the light beams sent by Alice expand significantly during the propagation, forcing Bob and Eve to use very large telescopes to collect the light efficiently. One can then argue that an air- or space-craft able to transport such big optical elements should be fairly easy to detect

along the line-of-sight between the parties. Assuming the use of some channel monitoring technique, like *RAdio Detection And Ranging* (RADAR) or *LIght Detection And Ranging* (LIDAR), one can bound the amount of light that Eve can collect from Alice and resend to Bob. On this ground, in a realistic threat model for satellite-based QKD one can consider that Eve has only limited access to the quantum link. In other words, she has access only to a lossy version of the signals sent by Alice and she is connected to Bob by a lossy channel as well.

A publication regarding the results of this project is currently in preparation. In this chapter we first review some of the main ideas of the work, in Sec. 5.1. Then, in Sec. 5.2, we report a simplified model to bound the transmittance of the quantum channels between Alice and Eve and between Eve and Bob, assuming different monitoring techniques. Finally, we address a side problem in Sec. 5.3, namely, the effect on the total link loss of the additional diffraction introduced by the presence of Eve's spacecraft along the line-of-sight.

5.1 Restricted eavesdropping and the effect on the key rate

The configuration of a satellite-to-ground optical link with eavesdropping is schematically represented in Fig. 5.1. Alice sends quantum signals towards the ground, where Bob's station is placed. Eve tries to tamper with the channel by collecting the light coming from Alice and sending new signals towards Bob. Eve might also decide to be passive, like in the right panel of Fig. 5.1, where she can only collect light but not feed her own signals into Bob's telescope, since she is on the ground too.

Optical links from low Earth orbit satellites are 500km long or more, so the correspondent light beams expand to several meters in diameter due to diffraction. In order to efficiently collect such light, Bob's and Eve's receivers must be very large. This im-

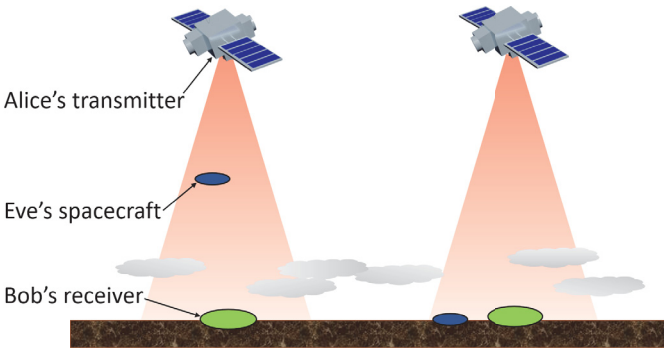

FIGURE 5.1: Scheme of satellite-to-ground optical link with eavesdropping, not to scale. Alice's transmitter is on the satellite and sends a light beam towards Bob's receiver aperture on the ground (green ellipse). Eve is on a spacecraft (blue ellipse) trying to tamper with the channel. The atmosphere, represented by clouds, only affects the link at the end of the propagation. In the panel on the left Eve is close to the line-of-sight and she can collect light and send it to Bob. On the right, instead, she is just passively collecting light from Alice.

plies that, in Fig. 5.1, Eve's vehicle must be large as well. Similarly, Eve needs a large telescope to send a collimated beam with a large beam waist and minimize its spreading. The preliminary estimations reported in Sec. 5.2 suggest that an object of that size along the line of sight between the parties Alice and Bob should be detectable by using monitoring techniques like RADAR or LIDAR. In this way we can bound the efficiency with which Eve can collect the light coming from Alice and inject light into Bob's apparatus. This situation can be modelled by imposing a lossy channel with transmissivity η_{AE} between Alice and Eve and assuming that the eavesdropper has no access to the signals lost. Similarly, a lossy channel with transmissivity η_{EB} connects Eve and Bob and again Eve has no access to the lost fraction of the

signals. This situation is portrayed in Fig. 5.2, where the lossy channels are simple represented as passing through a beam splitter with the proper transmissivity. Since the signals lost are not accessible to Eve, such losses can be considered trusted and incorporated into Alice's transmitter and Bob's receiver in the security analysis. This is the meaning of the extended boxes in Fig. 5.2. This situation is in contrast to the standard assumption in many QKD security proofs, in which Eve is free to substitute the actual links between her and the parties with ideal lossless channels, to implement her attacks. We point out that the simplified visualization given in Fig. 5.2 might not apply in every case, since it implies that all the signals arriving to Bob pass through Eve. This means that the cases corresponding to different values of η_{AE}, η_{EB}, η_{AB} (between Alice and Bob) and different protocols must be treated differently.

Figure 5.2: An eavesdropping model that accounts for a restricted Eve. Here, Eve receives Alice's signals with loss η_{AE}, and can send her signals to Bob with loss η_{EB}. Alice's and Bob's modules can be seen as extended encoder/decoder boxes.

We give now some hints on how these ideas influence some implementations of QKD. We choose as exemplary case the BB-84 protocol with single photons and weak coherent pulses. As we have discussed in Chap. 3, generally WCPs are used as approximation of single photons and tend to perform a bit worse, even employing the decoy state method. In this restricted eavesdropping scenario, the situation may be reversed. When using WCPs, the security of the communication usually requires to send coher-

ent states with mean photon number around one. In the scheme of Fig. 5.2, this requirement must be met at the exit of the extended Alice's box, because the loss corresponding to η_{AE} are trusted. This means Alice can send much more intense signals, with a mean photon number bigger than one at the output of her actual transmitter. This mechanism clearly does not work for single photon signals, so the limitation on Eve's power does not increase the achievable key rate. WCPs instead can achieve higher key rates, since the link can be made more efficient using signals with higher intensity.

Similar ideas can be applied to other discrete and continuous variable protocols [88, 89, 90], with very promising results. The ability to bound Eve's access to the QKD link, allowing less pessimistic assumptions in the security proofs, can improve significantly the performance of many QKD protocols.

5.2 Bounds on Eve's access to a satellite-to-ground link

As discussed above, traditional QKD assumptions includes the possibility that the eavesdropper can completely collect the light coming from the sender, manipulate it and forward it to the receiver without introducing losses. The two users are able to detect the presence of the eavesdropper simply by looking at the statistical properties of the sent and received signals, but this is achieved at the expense of the efficiency of the communication. While this can be considered necessary for fibre-based QKD, where the channel is partially underground and in locations that can be very difficult to monitor, it is an over-pessimistic assumption when considering free-space optical links. In such cases, in fact, the channel can be monitored using direct methods, such as RADAR, LIDAR or other imaging systems, to ascertain the presence of possible eavesdropping objects along the line-of-sight. In this section we bound the efficiency with which an hypothetical eaves-

dropper can collect and re-send QKD signals, if techniques for channel monitoring are employed in parallel. Such information can then be used inside the security analysis for *practical* satellite-based QKD.

In Sec. 5.2.1 we present the optical setup of the link with eavesdropping. Then some techniques for monitoring the channel are presented in Sec. 5.2.2. Finally bounds on the efficiency with which the eavesdropper can collect and re-send signals are showed and discussed in Sec. 5.2.3.

5.2.1 Optical setup of the link with eavesdropping

In this section we specify the optical setup used by the two authorised parties (Alice A and Bob B) for QKD and by the eavesdropper (Eve E) for the intercept-resend attack.

A is placed on a Low Earth Orbit (LEO) satellite, travelling in a circular orbit at altitude $L = 500$ km above the ground. It is equipped with a QKD source and a telescope with aperture radius $r_A = 15$ cm (like the Chinese satellite Micius [12]). B is instead placed on the surface of the Earth and he collects the light sent by A using a telescope with radius $r_B = 50$ cm. We address the static situation in which the satellite is at a fixed position right above the optical ground station, so that the length of the link is exactly L. We assume that E is represented by a spacecraft equipped with two telescopes, one for collection (pointed towards A) and one for transmission (towards B), both of radius r_E. We also assume, as a worst-case scenario, that the aperture of the telescope represents the whole projected area of E's spacecraft. In the following calculation we will allow E to have two distinct satellites, one for collecting and one for re-sending light, with appropriate values of the aperture radius and position. However, it turns out that the configuration of a single satellite is indeed optimal for her with the model used.

We assume that A's telescope sends the QKD signals in the form of a collimated Gaussian beam, with initial beam waist W_0

equal to the radius of the emitter telescope, at wavelength λ. For the light propagation we neglect the action of the atmosphere and the contribution of pointing errors. We use the standard expressions for Gaussian optics, corrected through the quality factor M^2 in order to replicate the far-field divergence of real optical elements [82]. E's telescope is instead perfect, meaning that she can send Gaussian beams with $M^2 = 1$. We point out that the use of W_0 equal to the radius of the emitter (utilized throughout the section) necessarily introduce truncation of the Gaussian beam, making it not perfectly Gaussian.

We identify with z the coordinate along the propagation path, so that A is at $z = 0$ and B at $z = L$. After a propagation length z, with $z \in [0, L]$, the beam width can be expressed as

$$W(z) = W_0 \sqrt{1 + \left(\frac{zM^2}{z_R} \right)^2} , \tag{5.1}$$

where $z_R = \frac{\pi W_0^2}{\lambda}$ represents the Rayleigh range of the beam. The comparison between the far-field divergence of a perfect Gaussian beam and the divergence measured for the Micius satellite suggests a value $M^2 \sim 3$. The transmittance of such a beam, when impinging at the centre of a circular collecting aperture of radius ρ can be expressed as

$$\eta(\rho, z) = 1 - \exp \left[-2 \frac{\rho^2}{W(z)^2} \right] \tag{5.2}$$

This expression can be used to compute the transmittance of A's beam through B's telescope, by setting $z = L$ and $\rho = r_b$

$$\eta_{AB} = 1 - \exp \left[-2 \frac{r_b^2}{W(L)^2} \right] , \tag{5.3}$$

which describes the efficiency of the QKD channel, apart from additional losses like atmospheric absorption, detection efficiency and transmittance of the optical elements. The same formula can

express the efficiency with which E can collect A's signals, if she is at position z and has a collecting aperture of radius $r_E(z)$

$$\eta_{AE}(z) = 1 - \exp\left[-2\frac{r_E(z)^2}{W(z)^2}\right]. \tag{5.4}$$

We supposed here that E is positioned exactly at the centre of the beam. The way we model the dependence of $r_E(z)$ on the distance from A and B will be specified in the next section.

We can use a similar approach to estimate the ability of E to re-send the signals that she intercepted towards B. In order to take full advantage of her optical system, we allow E to send focused beams. It was not necessary to take this into account in the case of A, because for this choice of the parameters the total propagation length L is much bigger than the Rayleigh range $z_R \sim 70$km, so focusing would not give any advantage. For the calculation we suppose that E has a lens of focal length f just in front of her sending aperture. After using the ray transfer matrix formalism one obtains the following expression for the width of a focused beam

$$W_E(z)^2 = \frac{\lambda^2}{\pi^2 r_E^2}\left[3\left(1-\frac{z}{f}\right)^2 d^2 + \left(1-\frac{z}{f}\right)^2 z_R^2 + z^2\right]. \tag{5.5}$$

E will optimize her strategy by always setting $f = z$, because it minimizes the width of the beam at z and so maximizes the transmittance through B's aperture. Notice that here r_E has the role of W_0. This results in a very simple expression for $W_E(z)$

$$W_E(z) = \frac{\lambda z}{\pi r_E(z)}, \tag{5.6}$$

which corresponds with Eq. 5.1 when $z \gg z_R$ and $r_E = W_0$. Now, using Eq. 5.2, we can compute the transmittance of E's beam through B's aperture

$$\eta_{EB}(z) = 1 - \exp\left[-2\frac{a^2}{W_E(z)^2}\right]. \tag{5.7}$$

We point out that, even in this case, the dependence of $r_E(z)$ over the distance A-E and E-B is very important and will be modelled in the next section.

5.2.2 Techniques for channel monitoring

In this section we want to put an upper bound on the size of E's spacecraft, depending on the distance from A's or B's position, if some sort of channel monitoring system is employed. Typical techniques are RADAR [91], LIDAR [92] and direct optical detection. We won't analyse the last one, as it requires rather stringent conditions: E's spacecraft must be illuminated by the sun while the receiver is in eclipse and the sky must be clear. A RADAR is very power-consuming, so we will address this technique as operated only from B, on the ground (even though examples of RADARs on spacecrafts can be found [93]). LIDARs instead require much less power and share similar optical elements as the one used for QKD, so may be placed on both A's and B's side.

We point out that the analysis reported in the following, especially for the LIDAR technique is very simplistic and several technical and physical details are neglected. So, the results are preliminary and a more complete analysis is in order. More advanced techniques, however, already developed in the LIDAR field, can be employed to improve these results, for example regarding background rejection and object recognition.

The performance of a RADAR is described by the so-called RADAR equation

$$z_{max} = \left(\frac{P_T G^2 \lambda \sigma}{P_{min} (4\pi)^3 k} \right)^{1/4}, \tag{5.8}$$

expressing the maximum distance at which an object with RADAR cross section σ can be detected. We are interested in the inverse

dependence $\sigma(z)$

$$\sigma(z) = \frac{P_{min}(4\pi)^3 k z^4}{P_T G^2 \lambda^2} \ . \tag{5.9}$$

Here P_{min} represents the minimum power measurable by the receiving system, P_T is the total power emitted, G is the gain of the RADAR antenna, k is a parameter that accounts for all the sources of additional losses.

The chosen values for the parameters are reported and discussed here:

- $G = \frac{4\pi\ 0.6\ \pi\ r_{ant}}{\lambda_R^2}$ where 0.6 is the antenna efficiency, $r_{ant} = 2$ m is the radius of the circular parabolic antenna and $\lambda_R = 4$ cm is the wavelength of the RADAR signals. We chose $r_{ant} = 2$ m as a reasonable size for a dish to be put alongside an optical ground station
- $P_T = 10^5$ W, as it is the power usually used in systems of this size (like the ones used in airports)
- $P_{min} = k_B T F_n B$, with k_B the Boltzmann constant, T the temperature, $F_n = 8$ dB is the so-called noise figure and $B = 2.5\ 10^6$ Hz is the effective noise bandwidth of the setup.
- $k = 7$ dB takes into account attenuation from atmospheric effects, filters and other sources.

In general the RADAR cross section σ is not equal to the geometric projected area and it strongly depends on the shape of the object. Only for spherical objects this two quantities coincide and this is the case we consider here. In this way, we can set the radius of E's telescope to r_E=$\sqrt{\sigma/\pi}$. The function in Eq. 5.9 for this values of the parameters is plotted in Fig. 5.3. Any value of r_E greater than the one in the graph would lead to a detection. We anticipate that the performance of the RADAR technique

are not sufficient to achieve interesting bounds on the transmittances η_{AE} and η_{EB} in Eq. 5.4 and Eq. 5.7. Even assuming that low-power RADAR or other techniques could be used to monitor the first tens of km around the satellite, a telescope of 3 m at 100 km from A would be able to intercept and resend with transmittances very close to 1. RADAR techniques are currently used to monitor the amount of objects present in low, medium and geostationary orbits around the Earth [94]. However, much bigger facilities (antenna radius $\sim$ 10 m) are necessary and the information is usually not available in real-time, but used to build and update catalogues of object.

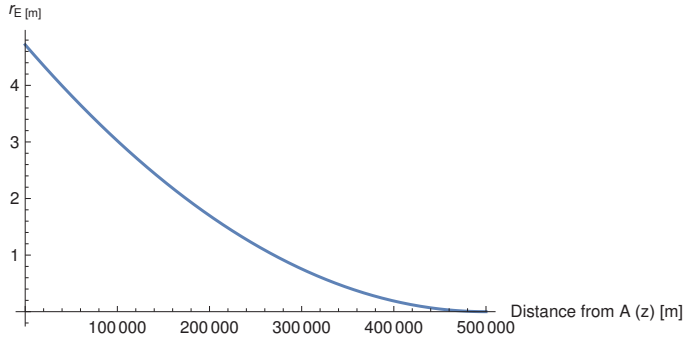

FIGURE 5.3: Maximum radius of E's telescope aperture as bounded from RADAR measurements.

A much higher performance/resources ratio can be achieved using LIDARs. The working principle is the same as with RADARs, but in this case light in the near UV - visible - near IR range is sent and recorded after reflection on the object under study. In this case, instead of enormous antennas, we only need telescopes of reasonable size, for example the same used for exchanging QKD signals. Instead of powers of tens of kW, lasers with 1 W power output are sufficient, meaning that this technique can rather easily be implemented on the satellite, as well as on B's side. As expected, the big advantage comes from the much shorter wave-

length of visible light with respect to the microwaves used in the RADAR technique, resulting in much smaller diffraction of the electromagnetic beam.

In this case, we can try to use again the standard RADAR equation of Eq. 5.9, with suitably chosen parameters. We report here a simple calculation, using again Gaussian optics, that gives an alternative result qualitatively similar to the RADAR equation. We use Eq. 5.6 and modify it to take into account the realistic quality factor M^2 estimated before

$$W_L(z) = \frac{\lambda_L z M^2}{\pi W_0} \,. \tag{5.10}$$

The intensity distribution of such a beam is Gaussian in the transversal plane and can be expressed as

$$I(r,z) = \frac{2P_T}{\pi W_L(z)^2} \exp\left[\frac{2r^2}{W_L(z)^2}\right], \tag{5.11}$$

where P_T is the total power carried by the beam and r is the distance from the beam centre in the plane transversal to the direction of propagation. We assume that the reflecting object is at the centre of the beam.

We compute the total power incident on the object integrating Eq. 5.11 in the area corresponding to E's spacecraft

$$P(z) = \int_{|r|<r_E} I(r,z) dr d\theta = P_T\left(1 - \exp\left[-\frac{2r_E^2}{W_L(z)}\right]\right) \tag{5.12}$$

Then we assume that the light is reflected back isotropically by the object under study, with albedo α

$$I_R(z) = \frac{P(z)\alpha}{4\pi z^2} = \frac{P_T \alpha}{4\pi z^2}\left(1 - \exp\left[-\frac{2r_E^2}{W_L(z)}\right]\right). \tag{5.13}$$

We considered here that the LIDAR transmitter and receiver are at the same coordinate and that the relative distance between

them and the object remains the same during the measurement. The total power collected is then $P_R(z) = I_R(z)\pi W_0^2 k$, where we introduced the total loss k encountered during transmission and collection. We can then invert this expression and equate $P_R(z)$ to the minimum power measurable by the receiving setup, to obtain the bound on the size of E's spacecraft

$$r_E(z)^2 = -\left(\ln\left[1 - \frac{2P_{min}kz^2}{\alpha P_T W_0^2}\right]\right)\left(\frac{\lambda_L z M^2}{\pi W_0}\right)^2 \qquad (5.14)$$

We set $\lambda_L = 800$ nm. We assume 50% loss in the optical system during transmission and collection, so $k = 1/(0.5^2)$. The transmitted power is set to $P_T = 1$W due to the limit on the power consumption on the satellite. For the ground-based LIDAR, this value could be exceeded easily (with maybe small advantage, see end of this section). We chose a rather conservative value for the albedo of the object, $\alpha = 0.1$, considering that for different metals it is usually around $\alpha = 0.5$ or more. Coating can be used to lower this value, however, measures at different wavelengths could maybe limit the effectiveness of this camouflaging technique. The estimated maximum radius of E's spacecraft that doesn't trigger our monitoring system is reported in Fig. 5.4. As before, any value of r_E greater than the one in the graph would lead to a detection. The results obtained with Eq. 5.14 and Eq. 5.9 are both reported. They differ because the efficiency of the transmitter and the reflectivity of the object are modelled in a different way. We are going to use Eq. 5.14 in the remainder of the section. We see that the bound on the size of undetectable objects is much smaller than what we obtained with the RADAR technique, giving hope that the transmittances computed in this case may be low enough to be useful for the enhancement of the security analysis.

The minimum measurable power P_{min} is in this case estimated as the background light collected by the satellite in normal working conditions. For the LIDAR placed on the satellite, the

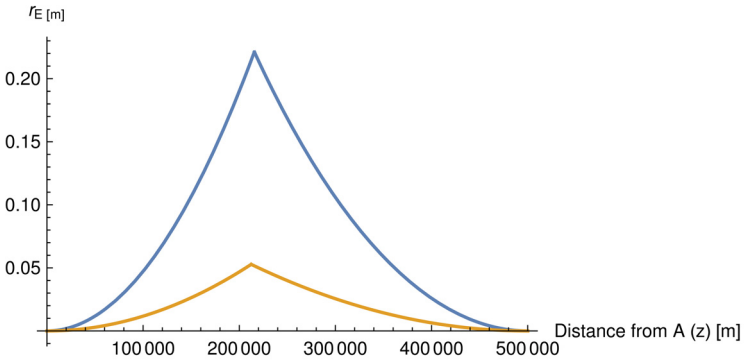

Figure 5.4: Maximum radius of E's telescope aperture as a function of z as bounded from LIDAR measurements, performed simultaneously from the satellite and from the ground. The bounds on this quantity obtained with two different techniques are reported: the blue curve corresponds to the LIDAR equation we deducted (Eq. 5.14), the orange curve to the RADAR equation (Eq. 5.9) with suitable parameters.

main background during night-time is represented by the light of the Moon reflected by the Earth [49]. It can be expressed as follows

$$P^A_{min} = \alpha_E \alpha_M R_M^2 r_A^2 \frac{\Omega_{fov}}{d_{EM}^2} H_{sun} B_{filter} \,, \tag{5.15}$$

where α_E and α_M are the albedo of Earth and Moon, R_M is the radius of the Moon, d_{EM} is the Earth-Moon distance, H_{sun} is the Sun irradiance at λ_L and Ω_{fov} is the field of view of the telescope and B_{filter} is the bandwidth of the spectral filters. For the LIDAR on the ground, we estimate the background light from the analysis in [87]

$$P^B_{min} = H_b \Omega_{fov} \pi r_B^2 B_{filter} \,, \tag{5.16}$$

where H_b is the brightness of the sky background. We point out that the analysis above regarding the minimum received power as-

sumes the sensitivity and low dark-count noise of a single-photon detector.

The previous analysis does not take into account the fact that the LIDAR detection from the ground will be strongly affected by the presence of the atmosphere. The air will back-scatter the light sent by B, especially when the sky is not completely clear, giving a signal that can cover the one expected from E's spacecraft. This means that, without additional analysis, every time we will measure a reflected power greater than P_{min}, we will think that E is there and we can bound her size. If part of the back-scattered light is due to the atmosphere, we will end up over-estimating her size and her collecting efficiency. The ability to detect the time-of-flight and reject the background, though, might make it possible to reconstruct E's presence anyway.

5.2.3 Bounds on Eve's transmittances

In this section we report the numerical results for E's collecting and re-sending efficiencies, obtained using the analysis performed in the previous sections.

We report in Fig. 5.5 the values of the transmittances between A and E and between E and B, computed from Eq. 5.4 and Eq. 5.7, as a function of z. In other words, these are the values of the transmittances that E can achieve if she positions here spacecraft at distance z from A. The maximum of both functions is achieved at the point where E's telescope can be the biggest. This happens because the widths of the beams, during the propagation, vary linearly with z, while the bound on E's size varies as z^2 (equivalently, the cross-section in Eq. 5.9 is proportional to z^4). We see that η_{AE} is kept below 0.1, while η_{EB} grows up to about 1. There are two main reasons for this behaviour: first, we allowed E to use perfect optics ($M^2 = 1$), that is, to generate Gaussian beams with minimal divergence and second, B's telescope aperture is bigger than A's.

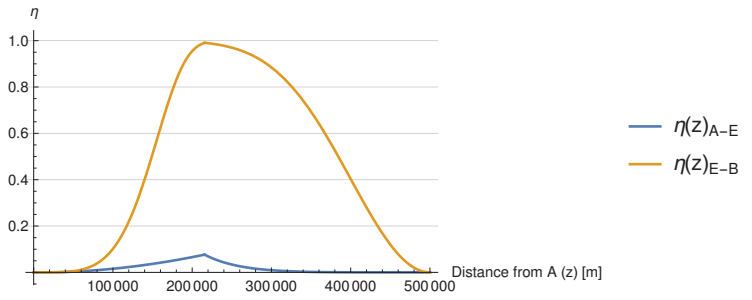

Figure 5.5: Values of η_{AE} and η_{EB} as a function of the coordinate z computed using Eq. 5.4 and Eq. 5.7.

We report in Fig. 5.6 the values of some quantities of the setup as a function of the distance z, useful to understand the behaviour observed in Fig. 5.5. The blue curve close to the x-axis is the same as the blue curve in Fig. 5.4, the maximum size of the undetected E. The green curve represents the width of the beam, sent by E at distance z with a telescope of radius $r_E(z)$, when it arrives at B's receiving plane. The orange curve is, instead, the width of the beam sent by A. We see that when it arrives at B after 500 km the beam is about $W(L) \simeq 2.5$ m in radius, giving a transmittance between the legitimate parties of about $\eta_{AB} = 0.05$ (only considering diffraction losses, without collection and detection losses). We have to compare this values to the minimum of the green curve, which gives $W_E \simeq 30$ cm at B and a transmittance of $\eta_{EB} \simeq 1$, as already pointed out.

The values in Fig. 5.5 can be lowered by raising the value of the transmitted power. Notice that $r_E \propto P_T^{1/2}$, so if we raise the power of a factor 4, to 4 W, the bound on E's size will be halved. In this case, much smaller values of η_{AE} and η_{EB} are expected, as shown in Fig. 5.7. η_{AE}, in particular, reaches a maximum of about 3 %, giving big room for improvement in the achievable key rate. This bounds are strongly dependent on the minimum measurable power P_{min}. Any improvement in the filtering tech-

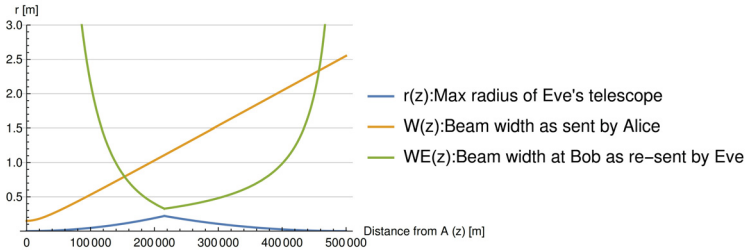

FIGURE 5.6: Values of some quantities of the setup as a function of the distance z, useful to understand the behaviour observed in Fig. 5.5.

niques (defined by the parameters B_{filter} and Ω_{fov}) will improve the performances. In the same way, going to lower wavelength will reduce the diffraction losses and improve the bounds.

We point out that the monitoring should be repeated with rather low frequency, let's say every second, leaving the remaining time for the QKD signal exchange. This means that the power actually consumed during this operation should be manageable even by rather small satellites.

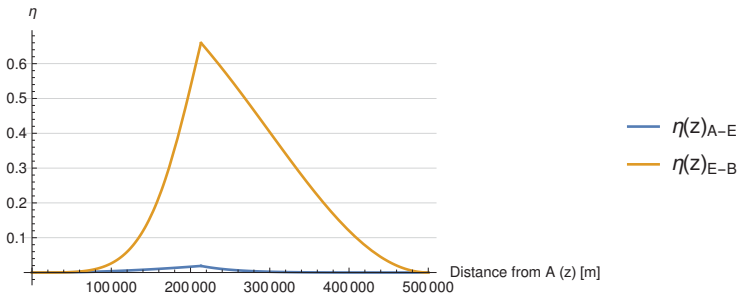

FIGURE 5.7: Values of η_{AE} and η_{EB} computed using Eq. 5.4 and Eq. 5.7, for a power of 4 W.

The LIDAR technique, with the simplified approach we used in these calculations, is sensible to the total power reflected by

objects illuminated by the transmitted light. This means that we are safe even in the situation where E places more satellites, which taken alone would be smaller than the detectable size. If we detect that an object or more are passing between A and B, by measuring a received power $P_R > P_{min}$, we can suppose that they are all malicious, estimate their size by replacing P_{min} with P_R in the expressions above and bound the transmittances in the real case.

We point out again that the presence of back-reflections from the atmosphere would give an over-estimation of the size of Eve when measured from B, which has not been considered here, leading to higher values of η_{AE} and η_{EB}. More sophisticated techniques should be able to address this problem, using the timing information obtained when using the LIDAR in the pulsed regime. The advantage introduced by sending a beam with higher power, analysed in Fig. 5.7 would be less effective for B, because it would correspond to more light back-reflected by the atmosphere, too.

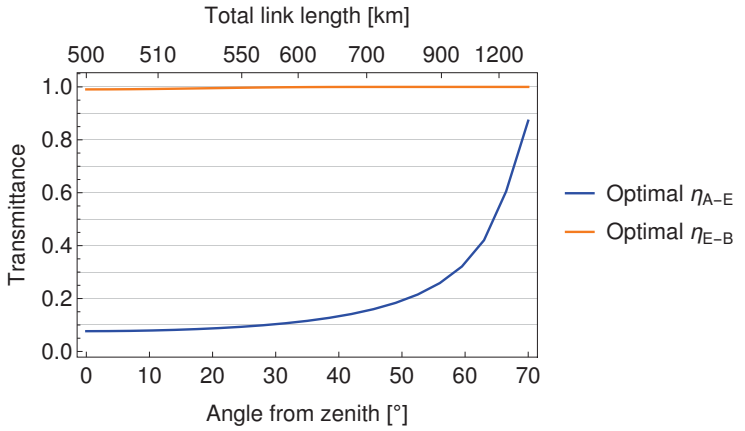

Figure 5.8: Maximum values of η_{AE} and η_{EB} as a function of the position of the satellite, for a LIDAR transmitted power of 1 W.

Until now we considered the static case where the satellite is

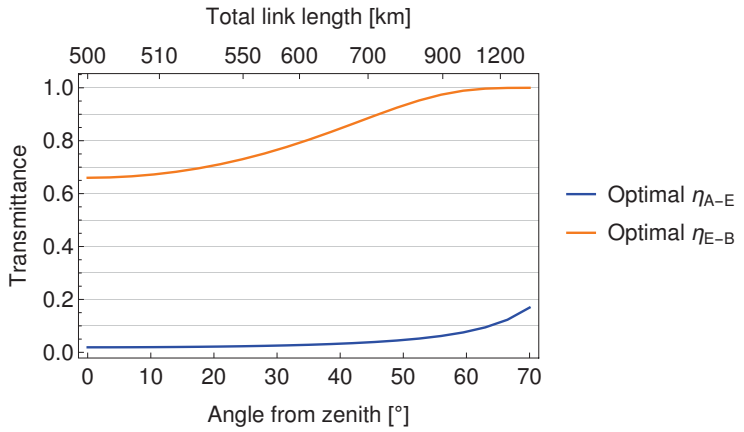

FIGURE 5.9: Maximum values of η_{AE} and η_{EB} as a function of the position of the satellite, for a LIDAR transmitted power of 4 W.

fixed at the position closest to the ground station. We study now how the maximum values of η_{AE} and η_{EB} (optimal for E) vary during the passage of the satellite. We show the results in Fig. 5.8 for P_T =1 W transmitted power from the LIDAR setup and in Fig. 5.9 for P_T=4 W. Both the configurations perform well regarding η_{AE} for high elevation angles (small angles from zenith), however the higher power level is required to put useful bounds at low elevation angles. As pointed out before, if the available power output is limited, one can achieve the same performances acting on other parameters of the setup.

In the previous analysis we fixed the reflectivity properties of E's spacecraft to bound its size. The value chosen at the end of Sec.5.2.2, $\alpha = 0.1$, is conservative enough if one considers standard spacecrafts, however much lower values of reflectivity parameters can be reached if specific technologies are used. For, example nano-structured coatings [95] can be laid over opaque surfaces, which ensure reflectivity values $< 10^{-2}$. Similar values

can be obtained on transparent surfaces (such as lenses), using multi-layer interferometric coatings. In Fig.5.10 we report the minimum value of reflectivity parameter of E's surfaces to achieve $\eta_{AE} < 0.95$, for different positions of the satellite with respect to the ground station. We mean that, keeping fixed all the other parameters, any value of reflectivity $\alpha < \alpha_{min}$ will lead to η_{AE} close to 1, so only values $\alpha > \alpha_{min}$ lead to useful bounds in our analysis.

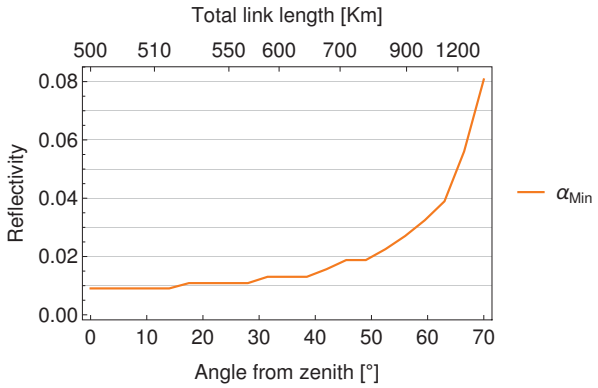

Figure 5.10: Minimum value of reflectivity parameter of E's surfaces to achieve $\eta_{AE} < 1$, as a function of the angle of the satellite with respect to the zenith of the ground station.

We see from Fig.5.10 that if E uses such high-performances coatings, the setup is not anymore sensible enough. In this case, we have to compensate for the lower reflectivity by increasing the emitted power P_T, increasing the directionality of the beam (smaller λ_L and/or bigger W_0) or decreasing the minimum measurable power P_{min}.

For comparison, we report in Fig.5.11 the behaviour of η_{AB}, from Eq.5.3, as a function of the position of the satellite. The red curve represents only the diffraction losses, while in the green curve the other sources of loss are also considered. In particular, 50% detection loss, 80% transmittance of the receiving optics and

absorption in the atmosphere $\chi_{ext} = \exp\big[-\beta \sec(\theta)\big]$, where $\beta = 0.7$ for $\lambda = 800$ nm and θ the angle from zenith (see [50, 17] for details). The inclusion of pointing errors should have a fairly small impact, about 2-3 dB. Note that the model used in this simulation in quite different from the one studied in Sec. 4.3, but the scaling is qualitatively similar.

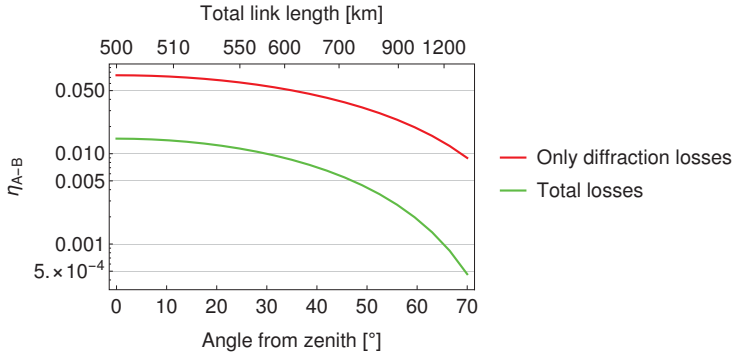

FIGURE 5.11: Transmittance of the beam sent by A through B's aperture η_{AB}, Eq.5.3, as a function of the position of the satellite.

5.3 Study of the additional diffraction introduced by Eve

We studied in the previous section (Sec. 5.2) how monitoring techniques, for example RADAR and LIDAR, can be introduced in a QKD setting, in order to put bounds on the efficiency with which Eve can collect signals from Alice and send signals to Bob. The two quantities have been identified with the transmittance of the channel A-E η_{AE} and of the channel E-B η_{EB}. At the end of the section we also estimated (in a simplistic manner) the transmittance of the total channel between the honest parties, η_{AB}, for comparison with the other two quantities.

However, the transmittance η_{AB} was computed in the absence of Eve, more precisely assuming a perfect line-of-sight link between A and B. The presence of an obstacle along the path, like the spacecraft used by Eve to collect and send the light, would introduce additional diffraction on top of the amount expected from just the propagation in free space and block some of the power of the beam.

In these notes we want to simulate the propagation of the diffracted beam and compare the results with the case of an unobstructed free-space link. In particular we assume that Alice sends a Gaussian beam with a given angular divergence along the z axis. Eve's spacecraft is represented by a disk, orthogonal to the direction of propagation and with centre on the z axis. Bob is instead modelled as a circular aperture orthogonal to the z axis and centred on it.

5.3.1 Fresnel diffraction due to a circular obstacle

The analysis performed here is similar to [96], but for a circular obstacle instead of an aperture. The scheme and the quantities involved are reported in Fig. 5.12.

The complex electric field distribution of a TEM_{00} Gaussian beam [82] can be expressed in the following way

$$U(r, z') = A\frac{w_0}{w}\exp\left(-\frac{r^2}{w^2}\right)\exp\left[ik\left(z' - \frac{r^2}{2R(z')} - \frac{\phi}{k}\right)\right]. \tag{5.17}$$

The amplitude has radial symmetry and r is the distance from the z-axis, the propagation direction. The distance from the beam's waist (corresponding to the transmitter plane) is indicated by z'. The amplitude A is connected to the intensity of the beam; w is the width of the beam and w_0 is the value at the beam waist, the narrowest point. The wave number is indicated by $k = 2\pi/\lambda$, with λ the wavelength of the light. ϕ is a phase factor and $R(z)$ is the radius of curvature of the wavefront.

We assume a circular obstacle of radius a with centre on the z-axis. The Huygens-Fresnel diffraction formula in the Fresnel approximation can be expressed as follows, taking advantage of the radial symmetry of the problem:

$$U(r,\phi,z) = \frac{1}{i\lambda z}\int_a^{\infty}\int_{-\pi}^{\pi} U(r_0,z_0) \exp\left[ik\left(z + \frac{r^2+r_0^2}{2z} - \frac{rr_0}{z}\cos(\theta-\phi)\right)\right] r_0 dr_0 d\theta \,. \tag{5.18}$$

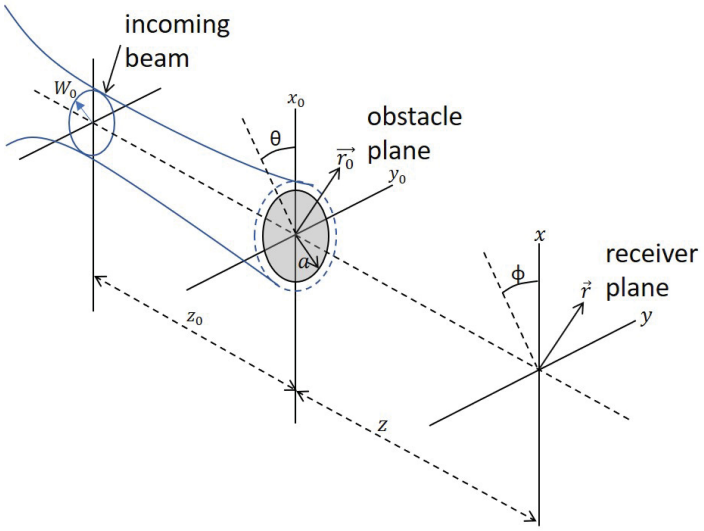

FIGURE 5.12: Schematic representation of the beam propagation with an opaque obstacle along the line-of-sight. The variables are described in the text.

As shown in Fig. 5.12, the variables r_0 and θ refer to the plane of the obstacle, while r and ϕ are in the receiver plane. $U(r_0, z_0)$ is the complex electric field at the obstacle plane, distant z_0 from the transmitter. The receiver plane is distant z from the obstacle

plane. The beam width and the radius of curvature of the wavefront can be written in the following way, as a function of the distance z'

$$w(z') = w_0\left[1+\left(\frac{\lambda z'}{\pi w_0^2}\right)^2\right]^{1/2} \qquad R(z') = -z'\left[1+\left(\frac{\pi w_0^2}{\lambda z}\right)^2\right]. \tag{5.19}$$

The angular integration in Eq. 5.18 yields a Bessel Function of the first kind of zero order $J_0(t)$, resulting in the following expression

$$U(r,z) = I\exp(i\beta)\int_a^\infty \exp(-r_0^2 C) r_0 J_0\left(\frac{krr_0}{z}\right) dr_0\ . \tag{5.20}$$

where we used these definitions

$$I = \frac{2\pi A}{i\lambda z}\frac{w_0}{w} \qquad B = k\left(z + z_0 + \frac{r^2}{2z} - \frac{\phi}{k}\right), \tag{5.21}$$

$$C = \frac{1}{w^2} + \frac{ik}{2}\left[\frac{1}{R(z_0)} - \frac{1}{z}\right]. \tag{5.22}$$

The beam width a the obstacle plane has been named $w = w(z_0)$ for clarity. We can now integrate by parts using the following relation for the Bessel functions

$$\frac{d}{dr}[r^{-n}J_n(\alpha r)] = -\alpha r^{-n} J_{n+1}(\alpha r)\ . \tag{5.23}$$

The integral in Eq. 5.20 can be computed as follows, introducing the quantity $\alpha = kr/z$ and renaming $r_0 \longrightarrow r$

$$
\begin{aligned}
&\left[\frac{-\exp(-r^2C)}{2C} J_0(\alpha r) \right]_a^\infty - \int_a^\infty \frac{-\exp(-r^2C)}{2C} \frac{d}{dr}\big[J_0(\alpha r)\big]\, dr = \\
&= \frac{\exp(-a^2C)}{2C} J_0(\alpha a) - \left[- \frac{\exp(-r^2C)}{(2C)^2} \frac{\alpha J_1(\alpha r)}{r} \right]_a^\infty + \\
&+ \int_a^\infty \frac{r\exp(-r^2C)}{(2C)^2} \frac{\alpha^2 J_2(\alpha r)}{r^2} dr = \\
&= \frac{\exp(-a^2C)}{2C} J_0(\alpha a) - \frac{\exp(-a^2C)}{(2C)^2} \frac{\alpha J_1(\alpha a)}{a} + \int_a^\infty ...dr \\
&= ... \qquad (5.24)
\end{aligned}
$$

If we keep applying the integration by parts in the same way we can turn the integral in Eq. 5.20 in an infinite sum containing Bessel functions of any order $J_n(t)$

$$
\frac{1}{2C} \sum_{n=0}^{\infty} \left(- \frac{\alpha}{2C} \right)^n \exp(-a^2C) \frac{J_n(\alpha a)}{a^n} \, . \qquad (5.25)
$$

In order to compute the intensity from the complex field $U(r, z)$, we have to compute its modulus squared. For this reason it is useful to divide the infinite sum into a real and imaginary part. We perform the following substitutions

$$
C = \frac{1}{w^2} + iV = M\exp(-i\beta) \qquad (5.26)
$$

where

$$
\begin{aligned}
V &= \frac{k}{2}\left[\frac{1}{R(z_0)} - \frac{1}{z} \right] \qquad M = \left[\left(\frac{1}{w^2} \right)^2 + V^2 \right]^{1/2} \\
\beta &= \tan^{-1}(-w^2 V) \, . \qquad (5.27)
\end{aligned}
$$

We also express the imaginary exponential functions inside the sum as $\exp(i\gamma) = \cos(\gamma) + i\sin(\gamma)$ and obtain

$$\frac{\exp(i\beta)}{2M}\sum_{n=0}^{\infty}\Big(-\frac{\alpha}{2M}\Big)^n\Big\{\cos(n\beta-a^2V)\exp\Big[-\Big(\frac{a}{w}\Big)^2\Big]\frac{J_n(\alpha a)}{a^n}+i\,\sin(n\beta-a^2V)\exp\Big[-\Big(\frac{a}{w}\Big)^2\Big]\frac{J_n(\alpha a)}{a^n}\Big\}=$$
$$=\frac{\exp(i\beta)}{2M}\Big(\mathrm{Re}+i\mathrm{Im}\Big)\,. \tag{5.28}$$

Here we defined the real and imaginary parts of the sum as

$$\begin{aligned} Re &= \sum_{n=0}^{\infty}\Big(-\frac{\alpha}{2M}\Big)^n\cos(n\beta-a^2V)\exp\Big[-\Big(\frac{a}{w}\Big)^2\Big]\frac{J_n(\alpha a)}{a^n} \\ Im &= \sum_{n=0}^{\infty}\Big(-\frac{\alpha}{2M}\Big)^n\sin(n\beta-a^2V)\exp\Big[-\Big(\frac{a}{w}\Big)^2\Big]\frac{J_n(\alpha a)}{a^n}\,. \end{aligned} \tag{5.29}$$

The intensity can finally be written as

$$I(r,z)=\frac{|I|^2}{4M^2}(\mathrm{Re}^2+\mathrm{Im}^2) \tag{5.30}$$

In Fig. 5.13 we plotted the intensity profile of the beam diffracted by the obstacle, in blue, compared to the same Gaussian beam in the absence of E, in orange. In order to make them comparable we fixed the initial power of the beams to the same value. In particular, we computed the integral of the intensity of the beams at the emitter plane and put the result equal to 1 to normalize. In this way we fixed the value of $|A|^2$, contained inside $|I|^2$ in Eq. 5.30.

The shape of the profile with the obstacle in Fig. 5.13 will change depending on the size of E (compared to the beam waist) and the distance between A, E and B. Fringes are clearly visible, produced by the constructive and destructive interference at the

receiver plane. For the range of parameters considered here, even though the obstacle stops the central spot of the beam, we still have a bright spot in the centre of the receiver, because of the constructive interference there.

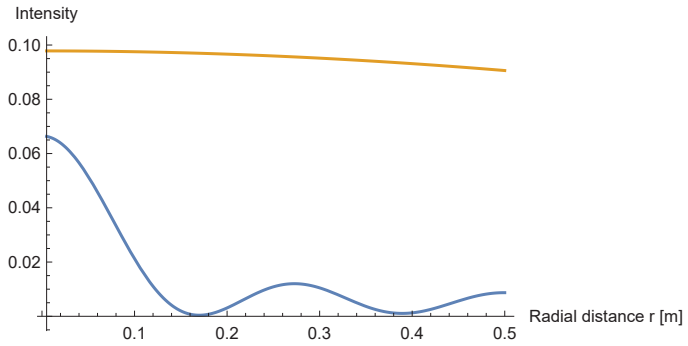

FIGURE 5.13: Intensity of the beam at the receiver plane (Bob) with (blue) and without (orange) the obstacle E, as a function of the radial distance from the z-axis. The radius of the obstacle has been fixed to 40cm for this example and W_0 to 15cm.

5.3.2 Application to the Alice-Eve-Bob satellite scenario

In this section we use the results about the intensity at the receiver plane to study the effects of the presence of Eve on the transmittance Alice-Bob η_{AB}.

The transmittance is simply defined as the integral of the intensity inside the aperture corresponding to Bob's telescope. We neglect absorption and turbulence in the atmosphere and losses related to coupling into optical fibres. Turbulence will also scramble the phase profile of the beam, changing the interference pattern observed. However, we point out that such effect will only be substantial for the final 10-20km of the link, so very close to the receiver on the ground. The radius of the receiving aperture

has been fixed to 50cm and the Gaussian beam waist is 15cm in the following. We assume a distance of $z + z_0 = 500$km between Alice and Bob (Low Earth Orbit satellite at zenith). We recall that in Sec. 5.2 the optimal size and position of Eve has been estimated using a model based on LIDAR detection. The corresponding values are approximately $a \approx 25$cm and $z_0 \approx 220$km from the blue curve in Fig. 5.4.

We show in Fig. 5.14 the transmittance as a function of the radius of the obstacle E (a in Fig. 5.12). The distance z_0 has been fixed to 220km and the vertical line corresponds to $a = 25$cm, the optimal values for Eve (as estimated in Sec. 5.2). We see that even a quite small obstacle introduces a significant increment in the total losses. These losses are due to two factors: 1) some of the power is blocked by the obstacle itself, 2) the additional diffraction makes the beam broader than without obstacle, increasing the geometrical losses.

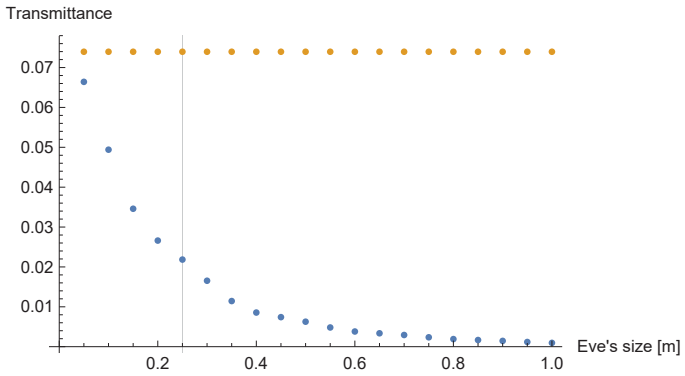

Figure 5.14: Transmittance through Bob's circular aperture with (blue) and without (orange) the obstacle E, as a function of the radius of the obstacle. The distance A-E has been fixed to 220km (optimal for Eve, as studied in Sec. 5.2). The vertical line marks the maximum size of Eve as estimated in Sec. 5.2.

In Fig. 5.15 we do the complementary analysis, fixing the size

of E to 25 cm and plotting the transmittance as a function of the distance A-E (z_0). The vertical line corresponds to the value $z_0 = 220$km.

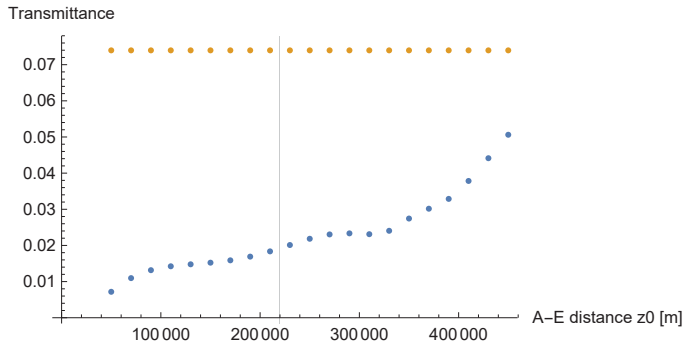

FIGURE 5.15: Transmittance through Bob's circular aperture with (blue) and without (orange) the obstacle E, as a function of the distance between Alice and Eve. The radius of E has been fixed to 25cm (optimal for Eve, as studied in Sec. 5.2). The vertical line marks the optimal distance A-E (220km) at which Eve achieves the highest η_{AE}, as estimated in Sec. 5.2.

The behaviour of the orange curve in Fig. 5.15 can be understood in the following way. The closer the obstacle is to the sender, the more power it blocks and the more diffraction it introduces, so the transmittance increases with the A-E distance z_0. The obstacle E (25cm) is smaller than the receiver aperture (50cm). So, even when it is close to it, a large fraction of the receiver remains un-obscured by the obstacle. That explains the fact that the transmittance keeps increasing. We report in Fig. 5.16 the same analysis for an obstacle of radius 50cm, as big as the receiver aperture. In this case, after the transmittance reaches a maximum, it starts decreasing, since the spot obscured by E covers entirely the receiver. The light that "bleeds in" due to diffraction on the edges is not enough anymore at longer z_0 to keep the transmittance high.

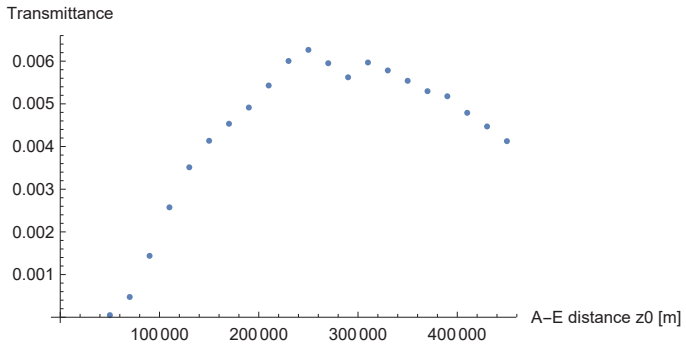

Figure 5.16: Transmittance through Bob's circular aperture in the presence of the obstacle E, as a function of the distance between Alice and Eve. The radius of E has been fixed to 50cm.

It's interesting to note the "bumps", particularly visible in Fig. 5.15 and Fig. 5.16 (and slightly visible in Fig. 5.14). They are due to the fact that, changing the size of E and the distance z_0, the positions of the minima and the maxima of the interference move. Sometimes they fall inside the receiver aperture and sometimes outside of it, producing the behaviour pictured in the graphs.

The case studied here is a very specific one, in which Eve is represented by a single circular object centered on the axis of propagation. Eve could also use, in principle, a set of smaller spacecrafts to collect the light. Such a configuration would clearly create a different diffraction pattern at the receiver plane. The calculation of the transmittance values in Sec. 5.2 are based on the same assumption.

We point out that these results should be considered in a different perspective with respect to what was found in Sec. 5.2. There, the quantities η_{AE} and η_{EB} cannot be measured during an experiment, so their values have been estimated to give an indication useful for the theoretical work discussed in Sec. 5.1. The transmittance η_{AB}, on the other hand, can be measured during

the experiment. One can estimate the expected transmittance with and without Eve. The actual transmittance of the link, however, is variable and sometimes altered by "invisible" factors (high-altitude clouds for example). This means that a value of the transmittance lower than expected cannot be directly linked to the presence of an eavesdropping spacecraft along the line-of-sight.

Introduction to Quantum Repeaters 6

We have already shown in the previous chapters how we can exploit satellite-based free-space optical links to achieve better loss-over-distance scaling with respect to fibre-based links. They allow to execute several quantum-enabled protocols over much longer distances than ground-based solutions. As we briefly reviewed at the end of Chapter 3, a great research effort has been put into the problem of enlarging the maximum distance of fibre-based implementations of QKD. A simple solution, based on trusted nodes, have already been utilised to build a quantum network that covers more than 2000km [57, 56]. First of all, a secret key is shared using QKD among the trusted nodes. The nodes perform a bit-wise XOR operation on the keys and broadcast the result. The parties can then easily reconstruct a common key. The main problem is that the nodes have full information about the key and so introduce weak links in the network that can be attacked by an adversary. What can be considered the ultimate solution is represented by the so-called Quantum Repeaters (QRs). The allow, in principle, to share entanglement over indefinitely long distances.

Quantum repeaters enable one to create a known entangled state between the end points of the network by first segmenting the network into pieces, creating entanglement between the segments and then finally connecting those entangled pairs to create the required long range correlation. This resource can then be used for a wide variety of quantum-enabled protocols. Quantum teleportation can be employed to transmit an unknown quantum state using the shared entangled pair. Quantum communication protocols like dense coding and untrusted-node QKD over very long distance can be enabled by quantum repeaters. Consuming entanglement, quantum metrology allows to achieve, in principle, higher precision in measurements than its classical counterpart. The same resource can also be used in distributed quantum computation or when a user wants to access a remote quantum server.

In this chapter we will, first of all, describe the three main ingredients necessary for a quantum repeater protocol to work (Sec. 6.1). An exemplary QR architecture is discussed in Sec. 6.2. Then, in Sec. 6.3, we will present the standard classification of quantum repeater protocols into three generations, characterised by increasing performance and technological difficulty.

In chapter 7 we will discuss how to integrate quantum repeaters with satellite-based links in order to achieve reliable entanglement distribution over global distances using a small number of untrusted intermediate nodes.

6.1 The components of quantum repeaters

The description of how a quantum repeater chain works in detail is postponed to Sec. 6.3. In this section we are going to analyse the three primary operations required to create long-range entangled states, in a generic quantum repeater protocol:

1. Entanglement distribution: the process of creating entangled links between elementary network nodes.

2. Entanglement purification: the process in which one creates an entangled state of higher quality from a number of lower quality ones.

3. *Entanglement Swapping* (ES): the process in which a Bell-state measurement is performed in a node on two halves of two separate Bell states. The Bell measurement allows to extend the entanglement, now existing between the two remaining qubits, by connecting two adjacent repeater links.

We will now briefly describe them independently, since they can be quite different in nature.

6.1.1 Entanglement distribution

Given two remote parties Alice (A) and Bob (B), entanglement distribution between them can be achieved in a number of ways, generally using photons as information carriers. The subject has already been addressed in the thesis but we mention here some aspects useful for the subsequent discussion about quantum repeaters.

We focus in particular on the mechanisms to entangle two remote matter qubits, for example atoms in a cavity, that we model as simple two-level systems. The nodes are connected by a quantum channel that we specify later.

The first scheme we address assumes that an optical Bell state $|\Phi^+\rangle_{p_1p_2}$, where

$$|\Phi^{\pm}\rangle_{p_1p_2} = \frac{|H\rangle_{p_1}|H\rangle_{p_2} \pm |V\rangle_{p_1}|V\rangle_{p_2}}{\sqrt{2}} , \qquad (6.1)$$

is being distributed to two adjacent nodes from a source located between them. Here p_1 and p_2 denote the two photons of the pair. The matter qubits in the nodes have been prepared in a superposition of the ground and excited states $|g\rangle$ and $|e\rangle$

$$|+\rangle_{a_i} = \frac{|g\rangle_{a_i} + |e\rangle_{a_i}}{\sqrt{2}} , \qquad (6.2)$$

where a_i denotes the i-th atom. At the arrival of the photon, a controlled-phase operation is applied on each atom-photon pair. The state of the atom inside the cavity is the control. A phase factor $e^{i\pi}$ is applied to the $|V\rangle$ component of the correspondent photon when the atom is in the $|e\rangle$ state. This operation results in the following overall state

$$|\Lambda\rangle = \frac{1}{\sqrt{2}} |\Phi^+\rangle_{a_1a_2} \otimes |\Phi^+\rangle_{p_1p_2} + \frac{1}{\sqrt{2}} |\Psi^+\rangle_{a_1a_2} \otimes |\Phi^-\rangle_{p_1p_2} \ , \tag{6.3}$$

with $|\Phi^\pm\rangle_{a_1a_2} = [|g\rangle_{a_1} |g\rangle_{a_2} \pm |e\rangle_{a_1} |e\rangle_{a_2}]/\sqrt{2}$ and $|\Psi^\pm\rangle_{a_1a_2} = [|g\rangle_{a_1} |e\rangle_{a_2} \pm |e\rangle_{a_1} |g\rangle_{a_2}]/\sqrt{2}$. Measuring the photons in the basis $|\pm\rangle = [|H\rangle \pm |V\rangle]/\sqrt{2}$, the post-measurement state of the atoms is in one of two Bell states depending on the results

$$|\Lambda'\rangle = \begin{cases} |\Phi^+\rangle_{a_1a_2} & \text{for } ++ \text{ or } -- \\ |\Psi^+\rangle_{a_1a_2} & \text{for } +- \text{ or } -+ \end{cases} . \tag{6.4}$$

The measurement results are announced to the other node and their parity reveal the Bell state shared.

We describe now a scheme that does not require a source of entangled photons. One of the two nodes, that acts as source, has prepared the atomic qubit in the state $|+\rangle_{a_1}$ and a single photon in $|+\rangle_p$. The photon interacts with the atom-cavity system through a controlled-phase operation (as before) and then sent over the channel to the adjacent node. There, it interacts in the same way with a qubit in the state $|+\rangle_{a_2}$. The total 3-qubit system is, as a result, in the state

$$|\pi\rangle = \frac{1}{\sqrt{2}} |\Phi^+\rangle_{a_1a_2} \otimes |+\rangle_p + \frac{1}{\sqrt{2}} |\Psi^+\rangle_{a_1a_2} \otimes |-\rangle_p \ . \tag{6.5}$$

Measuring again the photon in the $|\pm\rangle$ basis, the state of the matter qubits are projected onto $|\Phi^+\rangle_{a_1a_2}$ for a " + " detection and $|\Psi^+\rangle_{a_1a_2}$ for a " − " detection. The result is announced to the other node.

Both schemes succeed deterministically, if losses are neglected and the involved quantum operations are perfect. In general, one can express the probability of success of the remote entanglement generation between two nodes connected by an optical fibre of length L as

$$p_s = e^{-\alpha L} p_{\text{local}} \,, \tag{6.6}$$

where and we notice the exponential loss with attenuation parameter α, associated with the propagation in fibre, already introduced in Sec. 1.1 and at the beginning of Chap. 4. p_{local} is the probability of success of the local part of the protocol. In particular, $p_{\text{local}} = p_{\text{ent}} p_{\text{cou}}^2 p_{\text{det}}^2$ for the first scheme and $p_{local} = p_{\text{source}} p_{\text{cou}}^2 p_{\text{det}}$ for the second. Here, p_{ent} is the probability of emission of the entangled photons source, p_{cou} the coupling between the photon and the atom, p_{det} the detector efficiency and p_{source} the probability of emission of the single photon source.

6.1.2 Entanglement purification/distillation

The entangled states that one generates with a practical entanglement distribution scheme are never perfect, maximally entangled states. While losses can be overcome by attempting to generate the links many times, other errors will occur in such systems. Matter qubits can undergo dephasing even if they are long-lived and the same thing can happen to photonic qubits. Furthermore, our state preparation and detection may not be perfect. Such errors will in the end decrease the quality of the entangled link, or, in other words, decrease the fidelity F (defined in Sec. 2.1) with respect to the target Bell state (e.g., $|\Phi^+\rangle$). A generic noise model that describes well many real-life situations is white noise. The noisy state can then be written as a Werner state with fidelity F, that corresponds to a mixture of the target and the maximally mixed state or, equivalently, of all 4 Bell states:

$$\rho_w = \frac{1-F}{3}\mathbb{I}_4 + \frac{4F-1}{3} |\Phi^+\rangle \langle\Phi^+| \,. \tag{6.7}$$

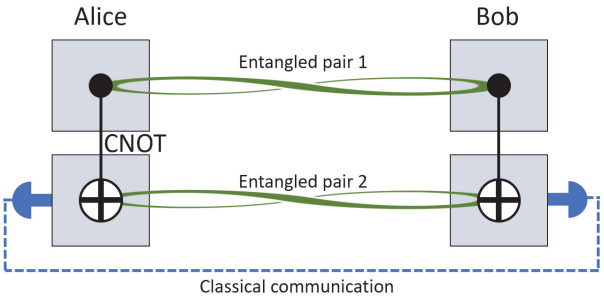

Figure 6.1: Schematic representation of a simple entanglement purification protocol with two imperfect Bell pairs, local CNOT operations, projective measurements and classical communication.

The decrease in fidelity means that information existing in the state has been lost and there is in general no simple way to recover it. However, since we are trying to generate a known Bell state, we can distil from multiple imperfect copies a Bell state with higher fidelity through a process known as quantum purification [97, 98]. The original scheme proposed by Bennet *et al.* [97] starts with two copies of the entangled pairs already established between the repeater nodes, as in Fig. 6.1. Within each node a CNOT operation is applied between the two local qubits. The two parties measure the qubits of one Bell pair in the computational basis $|0\rangle, |1\rangle$ and the results are broadcast. The resulting state is kept only if the measurement results are the same and in this case the protocol succeeded. A higher-fidelity state has been obtained as long as the initial fidelity of the pairs was above $F = 0.5$ and the local operations, CNOT and projective measurements, are not too noisy. The protocol failed if the results were different (0,1 or 1,0) and one needs to start over again distributing two fresh pairs. This aspect makes the protocol inherently probabilistic but heralded. If the initial entangled pairs are identical Werner states of fidelity F, the resulting state after

purification is still a Werner state but with a new fidelity value F_P

$$F_P = \frac{F^2 + \frac{1}{9}(1-F)^2}{F^2 + \frac{2}{3}F(1-F) + \frac{5}{9}(1-F)^2} , \qquad (6.8)$$

with a success probability equal to $P = F^2 + \frac{2}{3}F(1-F) + \frac{5}{9}(1-F)^2$. The constraint of using two identical states for purification can be relaxed, as in the so-called entanglement pumping protocol [18]. Accessory entangled pairs can be iteratively consumed to enlarge the amount of entanglement in a target system, however it is generally not possible to obtain maximally entangled states in this way.

The protocols discussed so far are simple examples of a two-way *Error-Detection Code* (EDC). A more advanced EDC and *Error-Correction Code* (ECC) can use multiple pairs of entangled states at the same time and can increase the fidelity with fewer iterations. As an example, a 5-qubit EDC can purify 5 imperfect pairs with a fidelity of 0.85 into one with fidelity above 0.99 in a single round with a success probability of 0.44. Significantly more resources and communication time are generally required if one uses the recurrence method of [97] or entanglement pumping.

Finally, the schemes detailed so far have assumed perfect local operations (CNOT gates and measurements). In any realistic system this will not be the case and the effect can be twofold: heralded errors (e.g., when probabilistic gates fail) and unheralded errors (e.g., measurements errors, imperfect gates). In the first case, the purification round failed and we need to start over again. In the second case, instead, we do not know whether the error occurred and thus the fidelity of our Bell state will be limited.

6.1.3 Entanglement swapping

After establishing high-quality entangled links between adjacent nodes, entanglement swapping is used to extend the range of the entanglement. This operation consists in a *Bell State Measure-*

ment (BSM) (introduced in Sec. 2.3) on a node connecting two adjacent entangled links. Let's assume two neighbouring links in the state $|\Psi^+\rangle_{12} \otimes |\Psi^+\rangle_{34}$. The labels indicate the four qubits involved. If a measurement in the Bell state is performed between the qubits 2 and 3 (belonging to two different pairs), the state of the qubits 1 and 4 is projected into the state $|\Psi^+\rangle_{14}$ up to a correction operation. The latter will be one of the four Pauli operations $\{I, Z, X, ZX\}$ on qubit 1 or 4, depending on the result of the Bell measurement, communicated by the middle node to the neighbours together with acknowledgement of the success.

The Bell pairs at the elementary link level are in general not perfect, for example one can consider a Werner state with fidelity F with respect to the target Bell state. After the entanglement swapping we still have a Werner state between qubits 1 and 4, with fidelity $F' = F^2 + (1-F)^2/3$. So, if $F \sim 1$ and we have 2^n elementary links, the fidelity decreases approximately as $F' \approx F^n$. This is were entanglement purification becomes necessary again.

Let's consider the example of qubits encoded in the polarization degree of freedom of single photons. In this case a very simple Bell measurement can be performed by letting the photons carrying qubit 2 and 3 interfere on a beam splitter. The photons at the two output ports are sent through two polarizing beam splitters and four single photon detectors. Two out of the four Bell states can be distinguished looking at the coincident clicks, so a maximum success probability of $1/2$ for the Bell state measurement is obtained. The scheme is pictured in Fig. 6.2.

6.2 The Duan-Lukin-Cirac-Zoller protocol

We are going to discuss now the so-called *Duan-Lukin-Cirac-Zoller* (DLCZ) protocol [99], based on atomic ensembles. This is one of the earliest proposals capable of entanglement distribution and swapping based on light-matter interaction. The $i-$th atom of the ensemble is prepared in the ground state $|g\rangle_i$. The

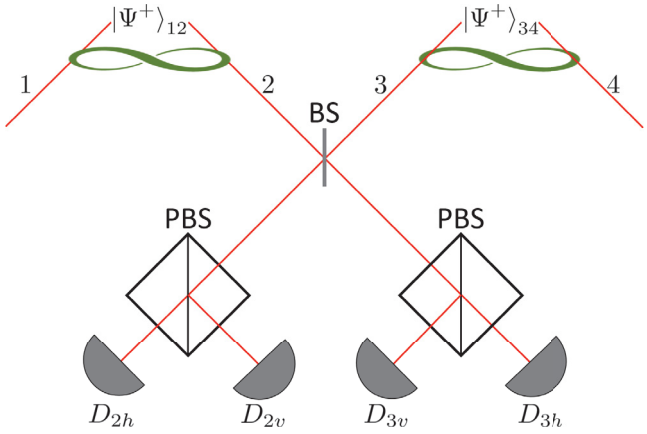

FIGURE 6.2: All-optical Bell state measurement. The entangled states $|\Psi^+\rangle$ are encoded in the polarization degree of freedom of single photons. The optical components used are: Beam splitter (BS), Polarizing Beam Splitter (BSM) and detectors D. If the proper coincident click pattern of the detectors is observed, the entanglement is swapped to modes 1 and 4.

systems also have another non-degenerate ground state $|\tilde{g}\rangle_i$ and an excited state $|e\rangle_i$. The energy level diagram of these three-level systems is pictured in Fig. 6.3.

A qubit can be represented by two collective states of the atomic ensemble, as follows

$$|0\rangle_{\text{ens}} = |g\rangle_1 |g\rangle_2 \cdots |g\rangle_N \qquad |1\rangle_{\text{ens}} = S^\dagger |0\rangle_{\text{ens}} \ , \tag{6.9}$$

where $S^\dagger = \sum_{i=1}^{N} |\tilde{g}\rangle_i \langle g| / \sqrt{N}$. An off-resonance laser pulse is used to induce potential Raman transitions from $|g\rangle$ to $|\tilde{g}\rangle$ and the emission of a photon from the $|e\rangle \rightarrow |\tilde{g}\rangle$ transition. If the pulse is weak, with mean photon number $n_p \ll 1$, the collective state of the ensemble can be written as

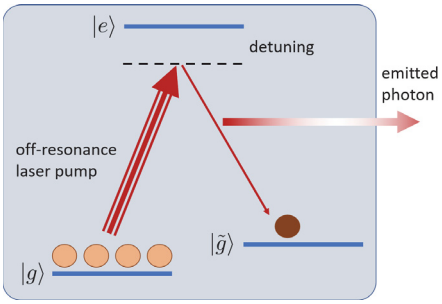

Figure 6.3: Schematic representation of the energy level diagram of the three-level systems composing the ensemble. It comprises two non-degenerate ground states $|g\rangle$ and $|\tilde{g}\rangle$ and an excited state $|e\rangle$.

$$|\tau_1\rangle = \sqrt{1-|\lambda|^2}(|0\rangle_{\text{ens}}|0\rangle_p + \lambda|1\rangle_{\text{ens}}|1\rangle_p + O(\lambda^2)) \,, \quad (6.10)$$

with $|\lambda| \ll 1$. Here the state $|0\rangle_p$ and $|1\rangle_p$ indicate, respectively, zero or one photons emitted. The state of two ensembles prepared in such a way can be remotely entangled with a simple procedure. The optical modes emitted from the two ensembles are let interfere in a 50/50 beam splitter. The overall state can be written as

$$|\tau_2\rangle \sim (1-|\lambda|^2)\{|0\rangle_A|0\rangle_B|0\rangle_{pA}|0\rangle_{pB} \quad (6.11)$$
$$+\lambda[|\Psi^+\rangle_{AB}|1\rangle_{pA}|0\rangle_{pB} + |\Psi^-\rangle_{AB}|0\rangle_{pA}|1\rangle_{pB}] + O(\lambda^2)\} \,,$$

where $\Psi^{\pm} = (|1\rangle_A|0\rangle_B \pm |0\rangle_A|1\rangle_A)/\sqrt{2}$. A and B label the two ensembles and pA pB the corresponding photonic modes. The state is projected onto $|\Psi^{\pm}\rangle_{AB}$ when a single photon is detected. Once such entangled states between remote ensembles are generated, they can be used in an entanglement swapping procedure. Since there is no direct way to perform a Bell measurement

between the ensemble-encoded qubits, the collective excitation is first coherently turned into a photonic one. The probabilistic and heralded Bell state measurement starts by exciting the $|\tilde{g}\rangle \rightarrow |e\rangle$ transition in one of the ensembles. The subsequent photon emission changes the total state into

$$|\Psi^+\rangle_{AB} \rightarrow 1/\sqrt{2}(|1\rangle_A |0\rangle_{pA} + |0\rangle_A |1\rangle_{pA}) |0\rangle_B \ . \quad (6.12)$$

The process is repeated for the other ensemble and the two optical modes are interfered on a beam splitter. The state of the four ensembles (two per entangled pairs) $\{A, B, C, D\}$ and correspondent photonic modes can be written as

$$\begin{aligned} |\tau\rangle &= \frac{1}{2}(|1\rangle_A |1\rangle_D |0\rangle_{pB} |0\rangle_{pC} \quad (6.13) \\ &+ \frac{1}{2\sqrt{2}}\{|1\rangle_A |0\rangle_D + |0\rangle_A |1\rangle_D\} |1\rangle_{pB} |0\rangle_{pC} \\ &+ \frac{1}{2\sqrt{2}}\{|1\rangle_A |0\rangle_D - |0\rangle_A |1\rangle_D\} |0\rangle_{pB} |1\rangle_{pC} \\ &+ \frac{1}{2\sqrt{2}} |0\rangle_A |0\rangle_D \{|2\rangle_{pB} |0\rangle_{pC} - |0\rangle_{pB} |2\rangle_{pC}\} \ . \end{aligned}$$

Upon detection of a single photon at the detectors, the state of ensembles A and D is projected onto either $|\Psi^+\rangle$ or $|\Psi^-\rangle$ (defined before). Some spurious terms would be present in case p_{cou} and p_{det} are not equal to 1. A classical signal has to be exchanged between nodes A and D to acknowledge success of this probabilistic procedure.

6.3 Quantum repeater protocols, fundamentals and classification

Generally, the structure of a quantum repeater chain is built as follows. The total communication distance L is divided into 2^n

segments of length $l = L/(2^n)$. The segments are connected by means of $2^n - 1$ repeater stations, placed at the intersection points, like in the top row of Fig. 6.4. The entangled links can be built as discussed in Sec. 6.1.1.

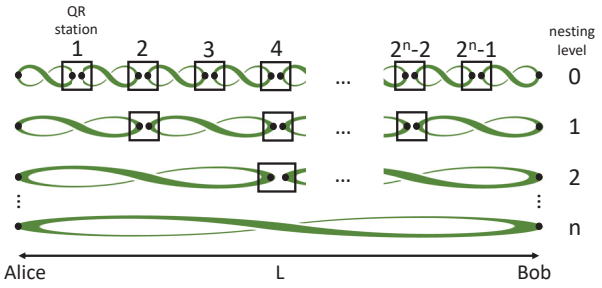

Figure 6.4: Schematic representation of a generic quantum repeater protocol based on the nested approach discussed in the main text. The green shapes indicate entangled links, the black dots the quantum memories and the black boxes the nodes performing the BSM.

In common repeater architectures the stations are equipped with quantum memories and an apparatus for entanglement swapping. A *Quantum Memory* (QM) consists in a device that allows to store the state of a flying quantum system (generally photonic) into a local static system. Promising platforms for this function are atoms in optical cavities and NV-centres in diamond [100].

After the entangled pairs are shared at the elementary link level, entanglement swapping is performed in order to connect two adjacent pairs. In consecutive *nesting levels*, the distance over which the entanglement is shared gets doubled. The end points of the chain are reached after n successful steps, with n the maximal nesting level. If the swapping is probabilistic, the procedure is repeated in a recursive hierarchical way to progressively extend the range of the entanglement, as shown in Fig. 6.4. If it is de-

terministic, instead, the swapping operations can be performed simultaneously. Entanglement purification can in principle be introduced at every level of the hierarchy. More details can be found in [101].

Based on the principles used to counteract losses and errors, three generations of quantum repeaters can be envisaged, each with specific strengths and technical requirements.

6.3.1 First generation

Let's assume a DLCZ-like protocol, composed of only entanglement generation and swapping and a network of total length L divided into 2^n elementary links. If losses are the only imperfection of the setup, the time required to successfully distribute a Bell state can be estimated as [102]

$$T_{\text{tot}} = \frac{L}{2^n c} \frac{f_0 f_1 ... f_n}{P_0 P_1 ... P_n} \frac{1}{P_s} \, . \tag{6.14}$$

We discuss this expression starting with the term $L/(2^n c P_0)$, with c the speed of light. It corresponds to the time necessary for an attempt to distribute an entangled state between two successive nodes, with success probability P_0, and acknowledge the success or failure. The terms f_i are related to the fact that before performing entanglement swapping, two entangled neighbouring links are necessary. The success probability of the entanglement swapping at the ith round is represented by P_i. P_s is the probability of successful post-selection at the end of the protocol. A useful approximation can be found as follows. Intuitively, if the waiting time for a single link is T, one only has to wait a time $T/2$ for a success in one of two neighbouring links. After that, one still has to wait a time T for a success in the second link. In this case the terms f_i can be approximated with $3/2$, as confirmed by numerical evidence [103]. The above expression can be rewritten as follows, expressing the terms P_0 and P_i on the basis of the theory introduced in Sec. 6.2

$$T_{\text{tot}} = \left(\frac{3}{2}\frac{1}{p_{\text{det}}p_{\text{cou}}}\right)^{(n+1)} \frac{L}{c|\lambda|^2 \mathrm{e}^{-\alpha l}} \,, \tag{6.15}$$

with $|\lambda| \ll 1$.

One can consider as additional imperfection, on top of losses, that a mixed state with fidelity $F < 1$ is distributed at the elementary link level. The fidelity of the resulting entangled link between the end nodes usually scales a F^{2^n} for a chain of 2^n links [19]. Entanglement purification can help to recover a higher fidelity. If this operation is performed between the end nodes, the time to generate one entangled pair is proportional to the round-trip time over the entire chain length, since classical signalling is required to herald the success in the purification protocol. The performance of practical matter qubits and quantum memories usually degrades exponentially with the waiting time L/c due to dephasing. So, the loss in fidelity scales exponentially with L. A similar reasoning can be applied if a probabilistic entanglement swapping procedure is used. The acknowledgement time is proportional to the total distance L and the exponential loss in fidelity appears again.

6.3.2 Second generation

As mentioned above, probabilistic entanglement purification or swapping conventionally necessitate two-way messaging. This fact creates a significant performance bottleneck, because of the waiting times for the classical messages saying whether the purification/swapping was successful. Moreover, if we consider the limited coherence of near-future matter qubits, it can make the scaling of the communication resources go back to exponential, as in the no-repeater case. Deterministic operations would allow to swiftly overcome such inconveniences. In the entanglement swapping protocol, for instance, one could assume to perform a deterministic Bell measurement. There exist, in fact, various

schemes with matter qubits that allow 2-qubit gates to be performed efficiently and faithfully. For entanglement purification, on the other hand, we have to exploit one-way schemes, that do not necessitate classical signals to indicate the success of the iteration. One can use error correction schemes to perform the purification [98], putting, however, significant constraints on the quality of the entangled links. As an example, the 5-qubit error correction code described in [104], assuming perfect local gates, has a threshold initial fidelity value of $F = 0.88$, below which the resulting purified state is more noisy than the initial pairs. The important advantage of this approach, however, is that the nodes do not have to wait for any classical message before the qubits can in the entangled links can be used again. This, in turn, has a massive impact on the required lifetime for the quantum memories, which is now of the order of the signalling time between adjacent nodes, instead of between the end nodes of the chain.

The overall performance of the chain can be further improved with the use of multiplexing. This addition also minimizes the required lifetime of the quantum memories. The number of attempts needed to successfully distribute an entangled pair between adjacent nodes can be estimated as

$$m_a = \frac{\log_e(\epsilon)}{\log_e(1 - p_s)} , \tag{6.16}$$

where p_s is the success probability of the entanglement distribution and $\epsilon \ll 1$ is the maximum failure rate. If this number of signals is sent in parallel, at least one link will be established with high probability. Clearly this method requires more resources, namely, additional sources and quantum memories at every node.

6.3.3 Third generation

The second generation quantum repeater schemes are ultimately limited in their achievable rates by the necessity to wait for the

classical signal that heralds the successful entanglement distribution in the elementary links. While this message is on his way, the qubits in those nodes are not available for further processing. Third generation repeater schemes try to significantly improve the performance of the network by avoiding this nuisance.

Loss-tolerant error correction codes can be used to encode the quantum signal [105]. In this case, when the full photonic encoded state is received by a node, it is transferred to matter qubits and loss events are heralded. The quantum state is corrected, reencoded with the full loss-tolerant code and transferred again to photons, which are sent further down along the chain. Such a scheme can tolerate only up to 50% loss in the elementary links, which corresponds to $\sim$ 15 km of standard telecom optical fibre. This means that hundreds of such repeaters are necessary to cover intercontinental distances. An important advantage of the scheme, however, is that the repeater nodes are only used to refresh the loss-tolerant code, so long-lived quantum memories are not necessary, unlike in the previous schemes. All the sources of waiting times that we discussed for the first and second generations are not present here, so the repetition rate is only limited by the slowest component in the chain.

In order to achieve polynomial scaling quantum repeaters, the matter qubits should satisfy all DiVincenzo's criteria for quantum computation [106]. Because of the difficulties inherent in building matter qubits of such high quality, all-optical alternative solutions have been devised that only rely on single-photon sources, detectors, linear optical elements and local active feedforward techniques. The time-reversed version of the DLCZ-like quantum repeater protocol has been used in [107] to develop an all-optical scheme. In the time reversal technique entanglement swapping and distribution at the elementary links level is simulated by means of optical cluster states. In a synchronised fashion, the source repeater nodes generate a photonic complete-like cluster state and then sends the two halves of it to the adjacent receiver nodes (Fig. 6.5). Then, the entanglement swapping is

completed by adaptive measurements in the Z and X bases. Several protocols have been proposed in which the resources (size of the cluster state) scale polynomially with the total communication distance. A very high repetition rates is in principle possible, as it is only limited by the local operations inside the repeaters.

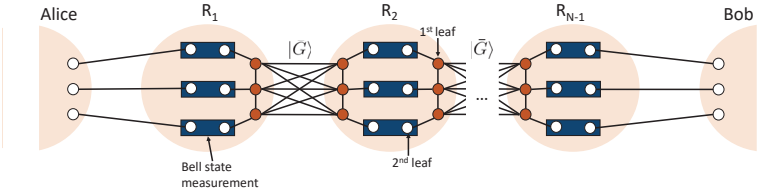

FIGURE 6.5: Simple representation of the all-optical repeater scheme. The cluster states $|\bar{G}\rangle$ has m left and right arms, composed of 1st and 2nd leaf qubits. The past application of a controlled phase gate is represented by an edge between the correspondent qubits. The cluster states are then used in the repeater protocol. Every source node prepares $|\bar{G}\rangle$ and the left (right) arms are sent to the correspondent adjacent receiver node R_i (R_{i+1}). Then R_i performs linear optical Bell measurements on the m pairs of 2$^{\text{nd}}$ leaf qubits received. It then measures in the (Z-basis) X-basis the 1$^{\text{st}}$ leaf qubits correspondent to (un)successful Bell measurements. The protocol fails if all the m Bell measurements fail. More details can be found in [19].

Integration of satellite-based links and Quantum Repeaters for quantum communication on a global scale 7

As discussed in the previous section, quantum repeaters have the potential to enable quantum communication over very long distances. They generally require, however, extremely high-quality quantum devices and resources to operate. Such technologies, like quantum gates with success probability very close to unity and extremely high-dimensional cluster states, might not be available for decades. So, a different approach should be devised for the medium-term future. The integration of quantum repeaters with satellite links can allow to reach global distances with a small number of nodes and quantum resources of lesser quality.

This chapter is organized as follows. In Sec. 7.1 we review some of the results of [20] (also in Sec. 9). We introduce the terminology and methods that we need for the successive sections, where we report some additional results not included in the paper. In Sec. 7.2.1 we specify how the orbits of the satellites have been

modelled in the simulations. In Sec. 7.2.2, instead, we analyse the dependence of the key rate on some important parameters of the setup, in particular the memory efficiencies, the radii of the telescopes and the height of the orbits.

7.1 Quantum repeaters in space

The material and the results described in this section are adapted from [20].

We have already introduced in Chap. 4 satellite-based links for quantum communication and how they can be utilized to cover much longer distances than what is currently achievable in fibre [12, 13, 14, 15]. Through quantum repeaters, few of these satellite links can be chained together to reach global distances. In [20] (also in Sec. 9) we proposed and studied the scheme pictured in Fig. 7.1, in which entanglement sources and quantum repeaters are placed on board of satellites, orbiting around the Earth in the *string of pearls* configuration. This allows to connect two users on the ground via free-space optical links outside the atmosphere, achieving far superior distance-to-loss ratio with respect to the standard fibre-based implementation. In this way, a small number of intermediate nodes is enough to achieve entanglement distribution over global distances at a reasonable rate.

The analysis is based on the first generation of quantum repeaters. The basic concept is the same already discussed in Chap.6: the total distance L between two trusted parties A and B is divided into 2^n elementary links. Entangled states are shared at the elementary link level and then entanglement swapping is applied to enlarge the range of the quantum correlations. The operation is repeated in a hierarchical way and, upon success in all the nodes and levels, finally an entangled state can be shared between the final ends of the chain, A and B. The parameter n is the maximal nesting level. More details can be found in [101, 20].

The elementary links can then be implemented in different

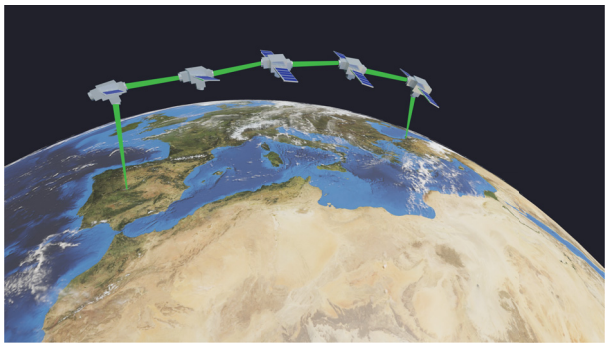

FIGURE 7.1: Pictorial representation of the scheme proposed in this paper for long-distance entanglement distribution, based on orbiting quantum repeater stations.

ways. In [20] we compare three different schemes. Scheme *Orbiting sources Orbiting repeaters* (OO) is the one we proposed, pictured in Fig. 7.1. Scheme *Orbiting sources Ground repeaters* (OG) has been proposed in [108] and extended to satellite constellations in [109]. Scheme *Ground sources Ground repeaters* (GG) is the standard fibre-based implementation. The three schemes are pictured in Fig. 2 of Chap. 9, to make the comparison clearer.

The quantum repeater platform considered here is based on quantum memories (QMs) and Bell state measurements (BSM) to store the quantum information and operate entanglement swapping. Quantum non-demolition (QND) measurement devices are used to herald the arrival of a photon at the repeater station. More details about the setting can be found in [20] (Sec. 9). The entangled quantum states shared at the end of the hierarchical entanglement swapping procedure can be used as resources for any quantum-enabled protocol, for example QKD. The key rate achievable when performing the BB-84 protocol, independently of the scheme used, can be expressed as follows

$$R_{QKD}^{BB84} = R_{\text{rep}}\, P_{\text{click}}\, R_{\text{sift}}\, r_{\infty}^{BB84}\,. \tag{7.1}$$

In the expression above, R_{rep} represents the entanglement distribution rate of the repeater chain, P_{click} the double detection probability, R_{sift} the sifting ratio (assumed equal to 1 in our asymmetric and asymptotic protocol) and r_{∞}^{BB84} the BB-84 secret fraction:

$$R_{\text{rep}} = \frac{1}{T_0} P_0 \, P_{QND}^2 \, P_W^2 \left(\frac{2}{3} P_{ES} \, P_R^2 \right)^n \tag{7.2}$$

$$P_{\text{click}} = \eta_d^2 \qquad r_{\infty}^{BB84} = 1 - h(e_Z) - h(e_X) \, . \tag{7.3}$$

In Eq. (7.2), the quantity $1/T_0$ represents the intrinsic repetition rate of the repeater architecture. We assume here that the memories used are highly multi-mode [110, 111] (see [108, 112] for additional discussion) so that we can avoid to wait acknowledgement from the adjacent stations that the photons have been received, before proceeding with the protocol or emptying the memory. This allows us to fix $T_0 = 1/R_s$, with R_s the repetition rate of the source (check Sec. 1.1 of [20] and footnote therein for details). The memory bandwidth of the chosen QM platform limits the maximum repetition rate, that we fix to 20 MHz for the following simulations [108, 113]. P_0 is the transmittance of the elementary links which depends on the scheme under study. We identify with P_0 the average of the link transmittance over one fly-by of the satellite for schemes OO and OG. P_{QND} is the efficiency of the QND measurement, P_W is the writing efficiency of the quantum memory, P_R is the reading efficiency of the quantum memory. P_{ES} is the success probability of the single entanglement swapping process (we refer to Sec. 3.1 of Chap. 9 and [101] for details). The term $2/3$ has been already discussed in Sec. 6.3.1. It arises due to a commonly employed approximation valid for small P_0, which is always valid in the cases under study (we refer to [114] for further details and the exact solution). In Eq. (7.3), η_d is the efficiency of the detectors used for the BB-84 measurements. The secret fraction r_{∞}^{BB84} depends, through

the binary entropy $h(p) = -p \log_2(p) - (1-p)\log_2(1-p)$, upon the error rates in the X and Z bases, e_X and e_Z. In our simulation they are estimated tracking the evolution of the state of the entangled pairs throughout the ES process. In a practical experiment these error rates are estimated during the parameter estimation stage, in which the parties make public a small subset of their measurement results and compare them.

In Fig. 3 of Chap. 9 we show the secret key rate, see Eq. (7.1), as a function of the total distance between the parties for several interesting configurations of schemes OO, GG and OG, in the range $[1000, 18000]$ km. We fix the altitude of the orbits at $h = 500$ km in schemes OO and OG. For the chosen values of the parameters $n \geq 4$ gives vanishing key rate so, in this range of distances, maximal ES nesting level $n = 2, 3$ are optimal. The newly proposed scheme (OO) performs better than the other configurations at every distance beyond ~ 1000 km, by orders of magnitude. A significant boost to the secret key rate and the maximum achievable distance results from the use of orbiting repeater stations. They allow to truly take advantage of the quadratic scaling of the transmittance with the distance that characterizes free-space optical links in vacuum, minimizing the negative effects of the atmosphere. In order to achieve non-zero key rate at the longest distance $n = 2$ is enough or, in other words, four source and 3 repeater satellites.

In [20] and Chap. 9 we also study the secret key rate for shorter distances (Fig. 4), compute the overpass duration for different configurations (Fig. 5) and analyse the performance on a 24-hours basis, to clarify the comparison with the ground-based implementation (Fig. 6 and Fig. 7). Furthermore, we also argue about the feasibility in the mid-term future (Sec. 1.2) and possible orbital configurations to fully utilize the potential of scheme OO (Sec. 1.3).

The results make it a promising candidate building block for a global quantum network, once such links are deployed using a satellite constellation and ground stations in suitable spots. Ad-

ditional studies are required, however, to examine the feasibility, cost and actual performance in concrete implementations.

7.2 Additional results

In this section we are going to describe additional results regarding the scheme described in this chapter, that were not included in [20].

First of all, in Sec. 7.2.1, we show how the orbits of the satellites were modelled and how the dynamical nature of the problem was handled. We compute the quantities used in the simulations presented in the paper, like the relative angles and distances between the satellites and the ground stations. Then, in Sec. 7.2.2 we analyse the dependence of the key rate on some important parameters, e.g., the memory efficiencies, the altitude of the orbits and the radii of the telescopes, for different choices of L and n.

7.2.1 Simulation of the orbits

In this subsection we will describe in detail how the orbits of the satellites were simulated to obtain the results in [20]. We also discuss how we computed the length of the different optical links and the elevation angles, that enter in the computation of the transmittance of the channels (Appendix of [20]).

The orbital configuration with the parameters necessary for the computation is schematically represented in Fig. 7.2. We consider circular orbits with altitude h above the surface of the Earth. The position of the satellite on the orbit is described by the vector $\vec{r}_A$ while the two ground stations correspond to B and C.

We focus first on a single downlink, used in scheme OO. The double downlink of scheme OG is analysed afterwards.

We name ϕ the angle between the y axis and the vector $\vec{r}_A$. θ, instead, corresponds to the angle between the y axis and the vector $\vec{r}$, corresponding to the elevation of satellite A with respect

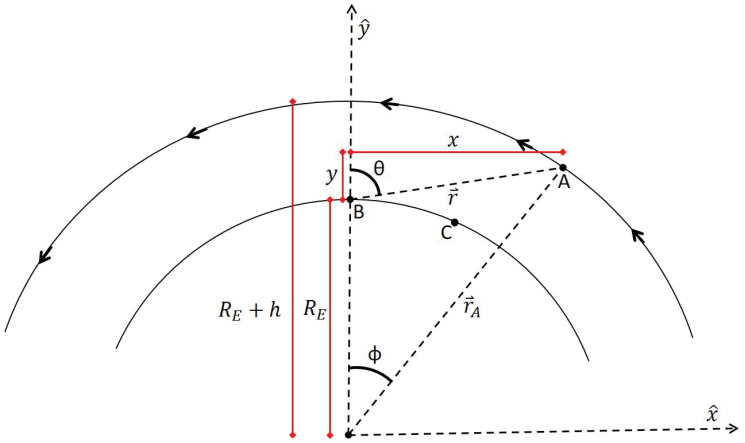

FIGURE 7.2: Schematic representation of the orbital configuration. The orbital plane corresponds to the $x - y$ plane. This is the nomenclature used: R_e radius of the Earth, h altitude of the circular orbits, ϕ the angle between the y axis and the vector $\vec{r}_A$ (which is the position of satellite A), θ the angle between the y axis and the vector $\vec{r}$.

to ground station B. The first step is to compute the relationship between the angular variables ϕ and θ. To do so, we express the quantity x in Fig. 7.2 as a function of ϕ and θ separately

$$x = \big(R_E + h\big)\sin(\phi) \qquad x = |\vec{r}|\sin(\theta)\ . \tag{7.4}$$

Now, we compute the modulus of the vector $\vec{r}$, the distance between the satellite and the ground station B. This is also one of the important quantities that enter in the computation of the transmittance of the downlink.

$$
\begin{aligned}
|\vec{r}| &= ||\vec{r}_A - \vec{r}_B|| = \sqrt{x^2 + y^2} = \\
&= \left\{ \left[(R_E + h)\sin(\phi) \right]^2 + \left[(R_E + h)\cos(\phi) - R_E \right]^2 \right\} = \\
&= \Big\{ (R_E + h)^2 \sin^2(\phi) + (R_E + h)\cos^2(\phi) + \\
&+ \quad R_E^2 - 2R_E(R_E + h)\cos(\phi) \Big\}^{1/2} = \\
&= \left\{ (R_E + h)^2 + R_E^2 - 2R_E(R_E + h)\cos(\phi) \right\}^{1/2} . \quad (7.5)
\end{aligned}
$$

We can then equate the two expressions of x and solve for $\sin(\theta)$, obtaining

$$
\sin(\theta) = \frac{x}{|\vec{r}|} = \frac{(R_E + h)\sin(\phi)}{\left[(R_E + h)^2 + R_E^2 - 2R_E(R_E + h)\cos(\phi) \right]^{1/2}} . \tag{7.6}
$$

We finally obtain the expression of θ as a function of ϕ

$$
\theta(t) = \arcsin\left\{ \frac{(R_E + h)\sin(\phi)}{\left[(R_E + h)^2 + R_E^2 - 2R_E(R_E + h)\cos(\phi) \right]^{1/2}} \right\} . \tag{7.7}
$$

We now introduce the dynamical aspect of the problem, assuming the following time dependence for the angle $\phi(t)$

$$
\phi(t) = \phi_0 + \frac{2\pi t}{T_S} \qquad \text{with } T_S = \frac{2\pi}{\omega \pm 2\pi/T_E} . \tag{7.8}
$$

Here ϕ_0 is just the initial value of the angle, T_S is the period of the revolution of the satellite, ω is the angular frequency of the orbit and T_E is the period of the rotation of the Earth. The

angular frequency can be computed as follows for stable circular orbits $\omega = \sqrt{\frac{GM_E}{(R_E+h)^3}}$, where G is the universal gravitational constant and M_E is the mass of the Earth. This relation is valid for circular orbits right above the equator and the $+/-$ sign correspond to orbits that co/anti-rotate with the Earth. For different orbital configurations the expression is slightly different but the numerical value is similar, since generally $\omega \gg \frac{2\pi}{T_E}$.

We define a fly-by of the satellite as the time it spends in contact with the ground station. We fix a minimum angle of $15°$ over the horizon, since more grazing angles are usually connected with too high loss and noise levels. The initial angle ϕ_0 is defined to be the one corresponding to the minimum angle $\theta_{min} = \theta(\phi_0)$. Then, the time evolution lead both angles to change, until we reach $\theta(t) = -\theta_{min}$. The elapsed time corresponds to the duration of the fly-by, for a single downlink. The values of θ and $|\vec{r}|$ are computed for every t to estimate the transmittance of the link (see Appendix of [20] for details).

For a double downlink we have to consider that both ground stations B and C need to be connected at the same time with the satellite A. This means that the satellite must have an elevation angle higher than θ_{min} with respect to both ground stations. In the next step we rotate the system by the angle $\alpha = l_{BC}/R_E$, where l_{BC} is the distance between the two ground stations on the surface of the Earth, as in Fig. 7.3.

The relation between the angular variables θ' and ϕ' is the same found before, with the additional conditions $\phi' = \phi - \alpha$ and so $\theta' = \theta(\phi') = \theta(\phi - \alpha)$. For the definition of the fly-by we proceed as before, with the difference that in this case both the angles θ and θ' must be in the interval $[-\theta_{min}, \theta_{min}]$.

For scheme OO an important quantity is the distance between two adjacent satellites, along the line of sight. It can be easily computed as

$$\tilde{L} = 2(R_E + h)\sin(\beta) \ , \tag{7.9}$$

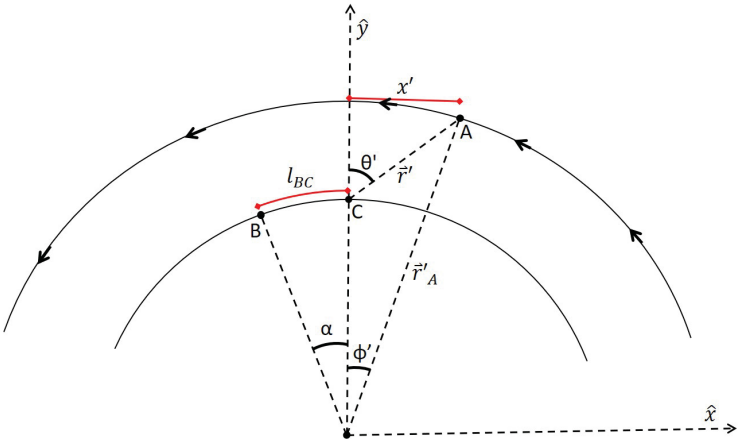

Figure 7.3: Schematic representation of the orbital configuration, after a rotation of the system by the angle α. ϕ' represents the angle between the y axis and the vector $\vec{r}'_A$, θ' the angle between the y axis and the vector $\vec{r}'$.

where β is the angular distance between the satellites. It depends on the altitude h, the total distance L and the maximal nesting level n.

We finally have the expression for all the quantities as a function of time. They are passed on to the function that computes the transmittance values for the different links. These quantities are then averaged over the time interval corresponding to the fly-by (as discussed in [20]).

7.2.2 Additional analysis of the key rate

In this subsection we further analyse the expression of the key rate formulas presented in the paper [20] and in Chap. 9. We focus in particular on its dependence on the memory writing and reading efficiencies, the telescopes radii and the altitude of the orbits.

First of all, we inspect the dependence of the key rate expres-

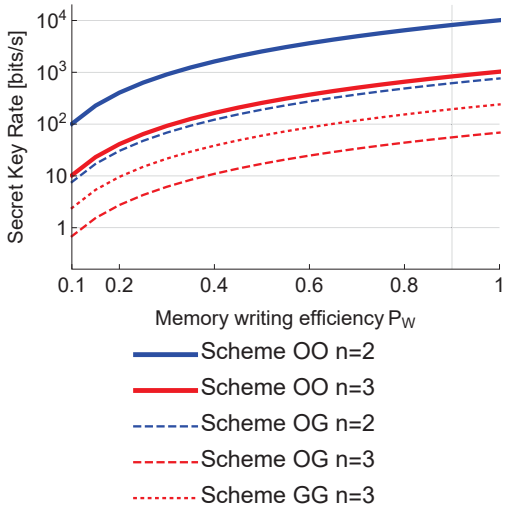

FIGURE 7.4: Key rate as a function of the memory writing efficiency P_W. We fixed the total distance to $L = 1000$km. The vertical line corresponds to the value of the writing efficiency used in the simulations in the paper [20] $P_W = 0.9$. The other parameters are kept fixed as reported in Tab.1 of [20].

sion (Eq. 7.1 and Eq. 7.2) on the memory writing efficiency P_W. We point out that exactly the same behaviour will be expected when varying the parameter P_{QND}. In Fig. 7.4 we report the key rate as a function of the writing efficiency P_W fixing the total distance to $L = 1000$km. The quadratic dependence is clearly visible and it is due to the fact that both qubits of the elementary entangled pairs must be successfully loaded into the memory for the protocol to proceed.

The same analysis is performed at a longer total distance $L = 8000$km and the results are reported in Fig. 7.5. In this case the GG scheme is not included since it gives zero key rate. As expected the behaviour is the same but the order of the curves is different, since scheme OG with $n = 2$ is getting close to the its

maximum range.

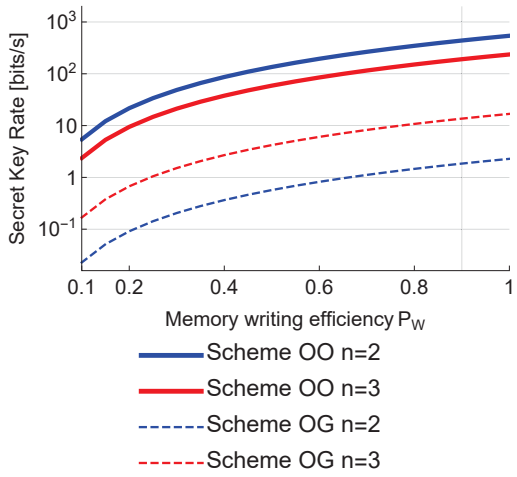

Figure 7.5: Key rate as a function of the memory writing efficiency η_R. We fixed the total distance to $L = 8000$km. The vertical line corresponds to the value of the writing efficiency used in the simulations in the paper [20] $P_W = 0.9$. The other parameters are kept fixed as reported in Tab.1 of [20].

The behaviour as a function of the memory reading efficiency P_R is more interesting, since it depends on n. As before, we study the key rate as a function of P_R in Fig. 7.6 fixing the total distance to $L = 1000$km. The different shape of the curves for different n is clearly visible and we also observe a crossing between the scheme OG with $n = 2$ and OO with $n = 3$. Lower values on n are favoured for memories with less efficient writing mechanisms.

We repeat the analysis for $L = 8000$km, out of the range of the ground implementation. The crossing this time happens between scheme OG with $n = 2$ and $n = 3$, even though, given the quite long distance, the implementation with $n = 2$ is better only for very inefficient memories.

Now we study how the key rate changes when the radii of

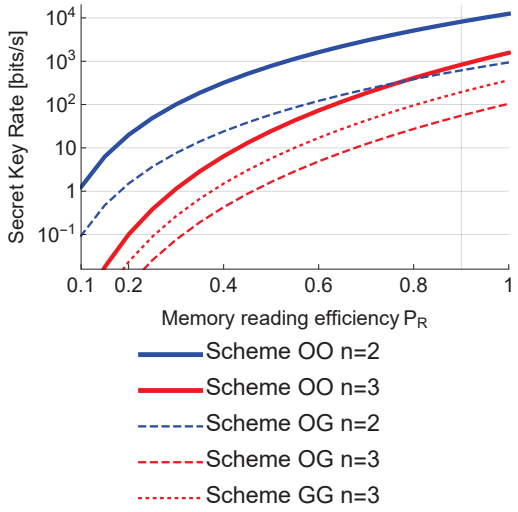

FIGURE 7.6: Key rate as a function of the memory reading efficiency P_R. We fixed the total distance to $L = 1000$km. The vertical line corresponds to the value of the reading efficiency used in the simulations in the paper [20] $P_R = 0.9$. The other parameters are kept fixed as reported in Tab.1 of [20].

the receiver telescope is varied. The results are showed in Fig. 7.8, for a total distance of $L = 8000$km. The key rate is reported as a function of the receiver radius for schemes OO and OG and for $n = 2, 3$. We point out that the same size of the receiver telescopes is considered everywhere, in the ground stations for scheme OG and OO and on the repeater satellites for scheme OO. The dependence of the single-link transmittance on the radius would be exactly quadratic if the receiver was illuminated by a uniform distribution of light. Since it receives roughly Gaussian beams with width much bigger than the aperture, the dependence is only roughly quadratic.

In Fig. 7.9 we report instead the key rate as a function of the Gaussian beam waist W_0, corresponding to the beam width

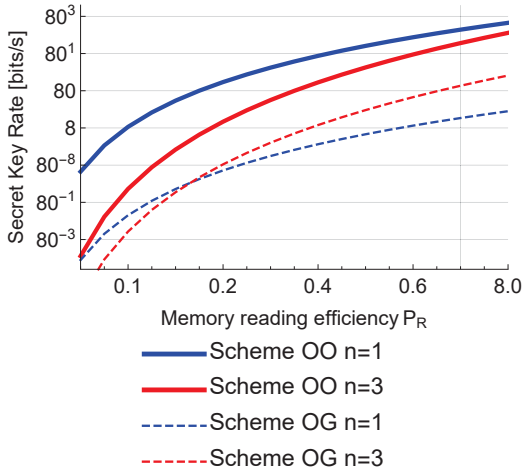

Figure 7.7: Key rate as a function of the memory reading efficiency P_R. We fixed the total distance to $L = 8000$km. The vertical line corresponds to the value of the reading efficiency used in the simulations in the paper [20] $P_R = 0.9$. The other parameters are kept fixed as reported in Tab.1 of [20].

at the transmitter. A very similar behaviour to the case studied above can be observed, even if the range of values on the x axis is different. We can conclude that telescopes much smaller than the ones assumed in the simulations in the main paper would still give a usable key rate and a significant advantage over the GG scheme.

The altitude of the circular orbits, as also discussed in [20], has two main effects on the performance of the repeater chain. On one hand, higher orbits ensure longer fly-by duration. They also allow, when using double downlinks, to connect much more distant ground stations, avoiding the negative effects of grazing incidence in the atmosphere. On the other hand, higher altitudes mean longer links, with additional losses. In this case we choose to show the total amount of secret key shared in a day, instead of

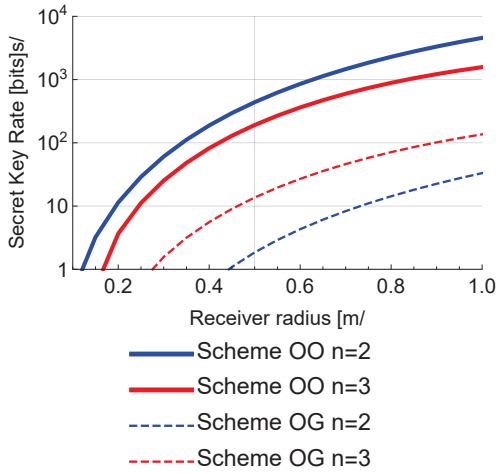

FIGURE 7.8: Key rate as a function of the radius of the receiver telescopes, in the ground stations and on the repeater satellites (for scheme OO). The vertical line corresponds to the value $R = 50$cm, used in the other graphs and in [20]. The other parameters are kept fixed as reported in Tab.1 of [20].

the key rate per second. It is simply computed, as also discussed in [20], by multiplying the average key rate by the duration of the fly-by, assuming a single pass per day. It's clear now how the conflicting effects listed above regarding the height of the orbits produce opposite results on this figure of merit.

In Fig. 7.10 the results for scheme OG are presented. It is clear how higher orbits lead to less key exchanged per day at short distances, since the longer fly-by duration can not make up for the much lower transmittance. At medium and long distances, however, the longer connection time and the higher elevation angles ensured by higher orbits allow to reach much longer distances. In particular, the maximum distance roughly doubles when going from $h = 500$km to $h = 2000$km.

The situation is quite different for scheme OO. Going to

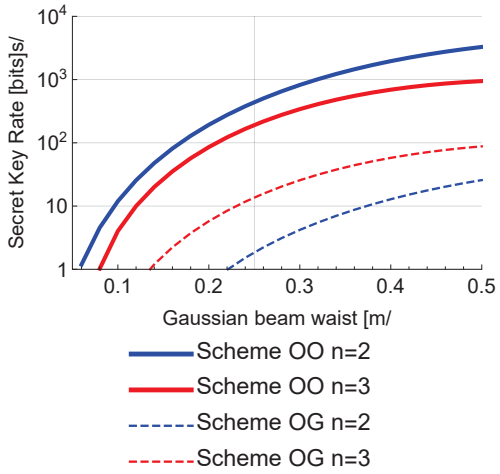

Figure 7.9: Key rate as a function of the Gaussian beam waist W_0, the beam width at the transmitter. The vertical line corresponds to the value $W_0 = 25$cm, used in the other graphs and in [20]. The other parameters are kept fixed as reported in Tab.1 of [20].

higher orbits has little to no advantage in this case. As expected, the lowest value of the altitude h that we examine (500km) is the best-performing one for a wide range of distances. Values around $h = 1000$km perform slightly better for distances longer than 14000km, thanks to the longer fly-by duration.

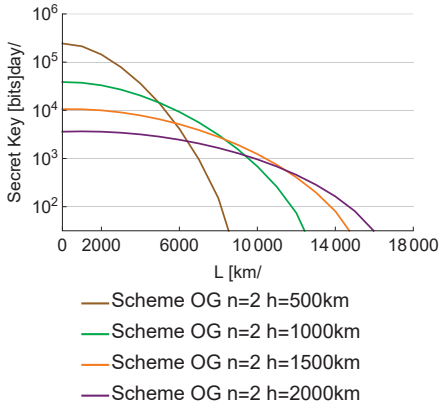

FIGURE 7.10: Key exchanged per day for different values of the altitude h of the circular orbits. We focus on scheme OG in this case. We remind that $h = 500$km was the standard value used in all the other graphs.

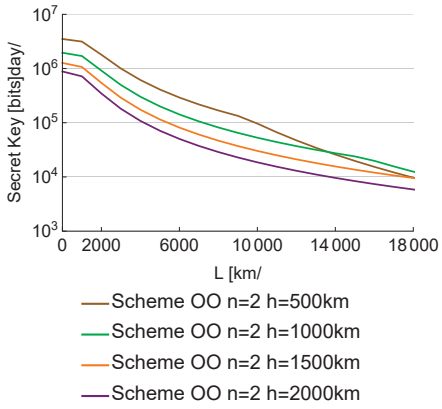

FIGURE 7.11: Key exchanged per day for different values of the altitude h of the circular orbits. We focus on scheme OO in this case. We remind that $h = 500$km was the standard value used in all the other graphs.

Contributions of the author 8

In this chapter we will specify the contribution of the author (CL) to the publications discussed in this thesis.

8.1 Satellite-based links for Quantum Key Distribution: beam effects and weather dependence

For this publication CL conceived the work and performed the analytical computations. CL also performed the numerical analysis and produced the figures. The author also discussed the results and wrote the draft.

8.2 Realistic threat models for satellite Quantum Key Distribution (in preparation)

The author computed the bounds on the efficiency of the free-space links between the parties and the eavesdropper. CL also performed the estimation of the effectiveness of different monitoring techniques. He also contributed to the discussions regarding the foundations of the work and its results. CL helped in the drafting of the paper and the final revision.

8.3 Quantum repeaters in space

The author proposed the scheme and analysed the pros and cons of it. CL executed the simulations of the orbits and the other physical parameters of the link. The author performed the analysis of the quantum repeater architecture and the computation of the secret key rate. CL produced the figures, drafted the paper and discussed the results.

Discussion and outlook 9

In this thesis we addressed different aspects of satellite-based quantum communication, with two main goals in mind. First of all, the development of tools to model such setups in a comprehensive and accurate way. A communication infrastructure based on a new paradigm will be expensive and challenging to build, so the expected performance of all the different components must be meticulously analysed in advance. Second of all, the study of innovative ways to take advantage of the new technology. Repurposing the already-existing global communication network to make room for quantum protocols might be the best solution in near future. In the long term, however, a more thorough reshaping of our global communication network might be necessary or at least advantageous. We don't have to wait a breakthrough in quantum communication to see this situation materialize, though. This topic, to a certain extent, is of great interest already right now. Companies like SpaceX have already started to use constellations of low Earth orbit satellites to bring broadband internet connection around the world, especially in isolated locations. Quantum

communication based on satellite constellations will end up sharing problems and criticism with such enterprises. Some concerns are: the effect of large satellite constellations on astronomic observations, collisions and the avalanche effect, space debris and its effect on future space exploration. Several countermeasures have been proposed but additional studies are necessary to ensure the viability of such solutions.

The analysis of the effects of turbulence on quantum light propagating in the atmosphere has been studied quite thoroughly, but the same cannot be said for the effect of other weather-related phenomena. The results discussed in this thesis in Chap. 4 represent a step in the correct direction, but extensive additional analysis is necessary to prove the viability of quantum communication in different atmospheric conditions. Innovative protocols might allow to overcome many of the difficulties introduced by the atmosphere. In this regard, studies specifically oriented towards particular implementations and encodings are necessary (e.g., polarization, time-bin or orbital angular momentum). A different route to solve the problem related to weather can be taken when networks are considered. The signals can be re-routed in the network to avoid the links affected by such issues, as considered for example in [115, 116].

When moving to new schemes and configurations, a critical re-evaluation of standard assumptions in quantum key distribution is always positive, like we did in Chap. 5. Another example is given by the development of hybrid protocols (e.g., [117]) that, giving up the information-theoretic security of standard QKD, achieve better performance by introducing assumptions based on computational hardness. This aspect is of particular interest if we consider that, in many practical cases, it is very difficult to ensure that all the assumptions of a QKD protocol are verified. In this perspective, imposing realistic restrictions on the eavesdropper looks more reasonable than in the ideal case. To turn QKD into a practically viable solution for long-range cryptography, this direction needs to be explored in detail.

The study of global communication networks based on satellite constellations have flourished in the last years (examples can be found in [115, 109, 116]). The scheme proposed in [20] ad discussed in Chap. 6 and Chap. 9 seems very promising for the building of a global quantum network but further analysis is required, to assess the performance in the field when a full constellation is deployed. The feasibility of such scheme also needs to be scrutinized in detail, since significant technical improvements over state-of-the-art experiments are necessary for its implementation. There is still much work to do to understand the potential of satellite-based quantum communication in applications in the field. In particular, the ability to distribute entanglement using double downlinks has been experimentally confirmed [13], but further development is necessary to make such operation more efficient. A cohesive study about hybrid quantum networks, built on the integration between satellite links and fibre networks on the ground is still to be attempted. Such a configuration seems complex and futuristic, but actually it has already been developed with trusted nodes [56] on a pretty large scale. The optimization of networks with such complex topologies is a central problem for the development of the future quantum internet.

List of Figures

List of Acronyms

Bibliography

[1] A. Yimsiriwattana and S. J. Lomonaco Jr. Distributed quantum computing: a distributed Shor algorithm. In *Quantum Information and Computation II*, volume 5436, pages 360 – 372. International Society for Optics and Photonics, SPIE, 2004.

[2] R. Van Meter and S. J. Devitt. The path to scalable distributed quantum computing. *Computer*, 49(9):31–42, Sep. 2016.

[3] M. P. Madhu and S. Dixit. Review on quantum computing tools and algorithms. In *Second International Conference on Computer Networks and Communication Technologies*, pages 714–719, Cham, 2020. Springer International Publishing.

[4] N. Gisin and R. Thew. Quantum communication. *Nature Photonics*, 1(3):165–171, 2007.

[5] M. Krenn, M. Malik, T. Scheidl, R. Ursin, and A. Zeilinger. *Quantum Communication with Photons*, pages 455–482. Springer International Publishing, Cham, 2016.

[6] V. Giovannetti, S. Lloyd, and L. Maccone. Advances in quantum metrology. *Nature Photonics*, 5(4):222–229, 2011.

[7] G. Tóth and I. Apellaniz. Quantum metrology from a quantum information science perspective. *Journal of Physics A: Mathematical and Theoretical*, 47(42):424006, oct 2014.

[8] E. T. Khabiboulline, J. Borregaard, K. De Greve, and M. D. Lukin. Optical interferometry with quantum networks. *Phys. Rev. Lett.*, 123:070504, Aug 2019.

[9] P. W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th Annual Symposium on Foundations of Computer Science*, pages 124–134, 1994.

[10] C.H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore*, pages 175–179, 1984.

[11] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299(5886):802–803, Oct 1982.

[12] S.-K. Liao et al. Satellite-to-ground quantum key distribution. *Nature*, 549:43 EP –, Aug 2017. Article.

[13] J. Yin et al. Satellite-to-ground entanglement-based quantum key distribution. *Phys. Rev. Lett.*, 119:200501, Nov 2017.

[14] J.-G. Ren et al. Ground-to-satellite quantum teleportation. *Nature*, 549:70 EP –, Aug 2017.

[15] J. Yin et al. Satellite-based entanglement distribution over 1200 kilometers. *Science*, 356(6343):1140–1144, 2017.

[16] R. L. Fante. Electromagnetic beam propagation in turbulent media: An update. *Proceedings of the IEEE*, 68(11):1424–1443, Nov 1980.

[17] C. Liorni, H. Kampermann, and D. Bruß. Satellite-based links for quantum key distribution: beam effects and weather dependence. *New Journal of Physics*, 21(9):093055, sep 2019.

[18] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller. Quantum repeaters: The role of imperfect local operations in quantum communication. *Phys. Rev. Lett.*, 81:5932–5935, Dec 1998.

[19] W. J. Munro, K. Azuma, K. Tamaki, and K. Nemoto. Inside quantum repeaters. *IEEE Journal of Selected Topics in Quantum Electronics*, 21(3):78–90, May 2015.

[20] C. Liorni, H. Kampermann, and D. Bruss. Quantum repeaters in space. *arXiv*, 2005.10146, 2020.

[21] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, USA, 10th edition, 2011.

[22] M. M. Wilde. *Quantum Information Theory*. Cambridge University Press, 2013.

[23] E. Schmidt. Zur theorie der linearen und nichtlinearen integralgleichungen. i. teil: Entwicklung willkürlicher funktionen nach systemen vorgeschriebener. *Mathematische Annalen*, 63:433–476, 1907.

[24] R. F. Werner. Quantum states with einstein-podolsky-rosen correlations admitting a hidden-variable model. *Phys. Rev. A*, 40:4277–4281, Oct 1989.

[25] M. Horodecki, P. Horodecki, and R. Horodecki. Separability of mixed states: necessary and sufficient conditions. *Physics Letters A*, 223(1):1 – 8, 1996.

[26] G. S. Vernam. Cipher printing telegraph systems for secret wire and radio telegraphic communications. *J. Amer. Inst. Elec. Eng.*, 45:pp.109–115, 1926.

[27] C. E. Shannon. Communication theory of secrecy systems. *The Bell System Technical Journal*, 28(4):656–715, 1949.

[28] P. J. Coles, M. Berta, M. Tomamichel, and S. Wehner. Entropic uncertainty relations and their applications. *Reviews of Modern Physics*, 89(1), Feb 2017.

[29] D. Yang. A simple proof of monogamy of entanglement. *Physics Letters A*, 360(2):249–250, Dec 2006.

[30] I. Devetak and A. Winter. Distillation of secret key and entanglement from quantum states. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 461(2053):207–235, 2005.

[31] V. Scarani and R. Renner. Quantum cryptography with finite resources: Unconditional security bound for discrete-variable protocols with one-way postprocessing. *Phys. Rev. Lett.*, 100:200501, May 2008.

[32] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner. Tight finite-key analysis for quantum cryptography. *Nat Commun*, 3:634, Jan 2012.

[33] N. Lütkenhaus. Security against individual attacks for realistic quantum key distribution. *Phys. Rev. A*, 61:052304, Apr 2000.

[34] W.-Y. Hwang. Quantum key distribution with high loss: Toward global secure communication. *Phys. Rev. Lett.*, 91:057901, Aug 2003.

[35] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo. Practical decoy state for quantum key distribution. *Phys. Rev. A*, 72:012326, Jul 2005.

[36] C. C. W. Lim, M. Curty, N. Walenta, F. Xu, and H. Zbinden. Concise security bounds for practical decoy-state quantum key distribution. *Phys. Rev. A*, 89:022307, Feb 2014.

[37] H.-K. Lo, M. Curty, and B. Qi. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.*, 108:130503, Mar 2012.

[38] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields. Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. *Nature*, 557(7705):400–403, May 2018.

[39] M. Minder et al. Experimental quantum key distribution beyond the repeaterless secret key capacity. *Nature Photonics*, 13(5):334–338, 2019.

[40] J. S. Bell. On the einstein podolsky rosen paradox. *Physics Physique Fizika*, 1:195–200, Nov 1964.

[41] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, 23:880–884, Oct 1969.

[42] U. Vazirani and T. Vidick. Fully device independent quantum key distribution. *Commun. ACM*, 62(4):133, March 2019.

[43] M. Epping, H. Kampermann, C. macchiavello, and D. Bruß. Multi-partite entanglement can speed up quantum key distribution in networks. *New Journal of Physics*, 19(9):093012, sep 2017.

[44] F. Grasselli, H. Kampermann, and D. Bruß. Conference key agreement with single-photon interference. *New Journal of Physics*, 21(12):123002, dec 2019.

[45] H.-L. Yin et al. Measurement-device-independent quantum key distribution over a 404 km optical fiber. *Phys. Rev. Lett.*, 117:190501, Nov 2016.

[46] J.-P. Chen et al. Twin-field quantum key distribution over 511 km optical fiber linking two distant metropolitans, 2021.

[47] A. Boaron et al. Secure quantum key distribution over 421 km of optical fiber. *Phys. Rev. Lett.*, 121:190502, Nov 2018.

[48] N. Sangouard, C. Simon, H. de Riedmatten, and N. Gisin. Quantum repeaters based on atomic ensembles and linear optics. *Rev. Mod. Phys.*, 83:33–80, Mar 2011.

[49] C. Bonato, A. Tomaello, V. Da Deppo, G. Naletto, and P. Villoresi. Feasibility of satellite quantum key distribution. *New Journal of Physics*, 11(4):045017, 2009.

[50] J.-P. Bourgoin et al. A comprehensive design and performance analysis of low earth orbit satellite quantum communication. *New Journal of Physics*, 15(2):023006, 2013.

[51] R. Bedington, J. M. Arrazola, and A. Ling. Progress in satellite quantum key distribution. *npj Quantum Information*, 3(1):30, 2017.

[52] R. Ursin et al. Entanglement-based quantum communication over 144 km. *Nature Physics*, 3(7):481–486, Jul 2007.

[53] S. Nauerth, F. Moll, M. Rau, C. Fuchs, J. Horwath, S. Frick, and H. Weinfurter. Air-to-ground quantum communication. *Nature Photonics*, 7(5):382–386, May 2013.

[54] P. Villoresi et al. Experimental verification of the feasibility of a quantum channel between space and Earth. *New Journal of Physics*, 10(3):033038, March 2008.

[55] H. Takenaka, A. Carrasco-Casado, M. Fujiwara, M. Kitamura, M. Sasaki, and M. Toyoshima. Satellite-to-ground quantum-limited communication using a 50-kg-class microsatellite. *Nature Photonics*, 11:502 EP, Jul 2017. Article.

[56] Y.-A. Chen. An integrated space-to-ground quantum communication network over 4,600 kilometres. *Nature*, 589(7841):214–219, Jan 2021.

[57] Beijing-shanghai quantum communication network put into use. http://english.cas.cn/newsroom/archive/news_archive/nu2017/201703/t20170324_175288.shtml. Accessed: 04-03-2020.

[58] T. Jennewein et al. QEYSSAT: a mission proposal for a quantum receiver in space. In *Advances in Photonics of Quantum Computing, Memory, and Communication VII*, volume 8997, pages 21 – 27. International Society for Optics and Photonics, SPIE, 2014.

[59] M. Payer. SES announces 10 project partners in quartz satellite cybersecurity consortium. https://www.ses.com/press-release/ses-announces-10-project-partners-quartz-satellite-cybersecurity-consortium. 2019.

[60] Pultarova T. Unleashing quantum into the world. https://eandt.theiet.org/content/articles/2019/04/unleashing-quantum-into-the-world/. 9-6-2019.

[61] E. Kerstel et al. Nanobob: a cubesat mission concept for quantum communication experiments in an uplink configuration. *EPJ Quantum Technology*, 5(1):6, Jun 2018.

[62] R. Haber, D. Garbe, S. Busch, W. Rosenfeld, and K. Schilling. Qube - a cubesat for quantum key distribution experiments. 2018.

[63] Science and technology facilities council. uk and singapore collaborate on £10m satellite project to develop next generation communications networks. https://stfc.ukri.org/news/uk-and-singapore-collaborate-on-10m-satellite-project/. 9/6/2019.

[64] D. K. L. Oi et al. Cubesat quantum communications mission. *EPJ Quantum Technology*, 4(1):6, Apr 2017.

[65] J. A. Grieve, R. Bedington, R. C. M. R. B. Chandrasekara, and A. Ling. Spooqysats: cubesats to demonstrate quantum key distribution technologies. 10 2017.

[66] S. P. Neumann et al. Q3sat: quantum communications uplink to a 3u cubesat-feasibility & design. *EPJ Quantum Technology*, 5(1):4, Apr 2018.

[67] E. L. Shkolnik. On the verge of an astronomy cubesat revolution. *Nature Astronomy*, 2(5):374–378, 2018.

[68] A. Poghosyan and A. Golkar. Cubesat evolution: Analyzing cubesat capabilities for conducting science missions. *Progress in Aerospace Sciences*, 88:59 – 83, 2017.

[69] W. A. Shiroma et al. CubeSats: A bright future for nanosatellites. *Central European Journal of Engineering*, 1:9–15, March 2011.

[70] V. I. Tatarskii. *The effects of the turbulent atmosphere on wave propagation*. Jerusalem: Israel Program for Scientific Translations. 1971.

[71] L. C. Andrews and R. L. Phillips. *Laser Beam Propagation through Random Media, Second Edition*. SPIE Press, 2005.

[72] F. Dios, J. Recolons, A. Rodríguez, and O. Batet. Temporal analysis of laser beam propagation in the atmosphere using computer-generated long phase screens. *Opt. Express*, 16(3):2206–2220, Feb 2008.

[73] F. Dios J. Recolons. Accurate calculation of phase screens for the modelling of laser beam propagation through atmospheric turbulence, 2005.

[74] Y. Cao, S. L. Dvorak, X. Ye, and B. Herman. A new cylindrical phase screen method for modeling electromagnetic wave propagation through an inhomogeneous 2-d atmosphere. *Radio Science*, 42(4).

[75] R. G. Lane, A. Glindemann, and J. C. Dainty. Simulation of a kolmogorov phase screen. *Waves in Random Media*, 2(3):209–224, 1992.

[76] C. M. Harding, R. A. Johnston, and R. G. Lane. Fast simulation of a kolmogorov phase screen. *Appl. Opt.*, 38(11):2161–2170, Apr 1999.

[77] E. Limpert, M. Abbt, and W. A. Stahel. Log-normal Distributions across the Sciences: Keys and Clues. *BioScience*, 51(5):341–352, 05 2001.

[78] A.N. Stassinakis, H.E. Nistazakis, K.P. Peppas, and G.S. Tombras. Improving the availability of terrestrial fso links over log normal atmospheric turbulence channels using dispersive chirped gaussian pulses. *Optics & Laser Technology*, 54:329 – 334, 2013.

[79] R. L. Phillips A. Al-Habash, L. C. Andrews. Mathematical model for the irradiance probability density function of a laser beam propagating through turbulent media. *Optical Engineering*, 40:40 – 40 – 9, 2001.

[80] N. D. Chatzidiamantis, H. G. Sandalidis, G. K. Karagiannidis, S. A. Kotsopoulos, and M. Matthaiou. New results on turbulence modeling for free-space optical systems. In *2010 17th International Conference on Telecommunications*, pages 487–492, April 2010.

[81] D. Vasylyev, A. A. Semenov, and W. Vogel. Atmospheric quantum channels with weak and strong turbulence. *Phys. Rev. Lett.*, 117:090501, Aug 2016.

[82] A. E. Siegman. Defining, measuring, and optimizing laser beam quality. In Anup Bhowmik, editor, *Laser Resonators and Coherent Optics: Modeling, Technology, and Applications*, volume 1868, pages 2 – 12. International Society for Optics and Photonics, SPIE, 1993.

[83] D. Vasylyev et al. Free-space quantum links under diverse weather conditions. *Phys. Rev. A*, 96:043856, Oct 2017.

[84] X.-B. Wang. Beating the photon-number-splitting attack in practical quantum cryptography. *Phys. Rev. Lett.*, 94:230503, Jun 2005.

[85] H.-K. Lo, X. Ma, and K. Chen. Decoy state quantum key distribution. *Phys. Rev. Lett.*, 94:230504, Jun 2005.

[86] X.-B. Wang, T. Hiroshima, A. Tomita, and M. Hayashi. Quantum information with gaussian states. *Physics Reports*, 448(1):1 – 111, 2007.

[87] E.-L. Miao, Z.-F. Han, S.-S. Gong, T. Zhang, D.-S. Diao, and G.-C. Guo. Background noise of satellite-to-ground quantum key distribution. *New Journal of Physics*, 7(1):215, 2005.

[88] F. Grosshans et al. Quantum key distribution using gaussian-modulated coherent states. *Nature*, 421(6920):238–241, Jan 2003.

[89] R. Renner and J. I. Cirac. De Finetti representation theorem for infinite-dimensional quantum systems and applications to quantum cryptography. *Phys. Rev. Lett.*, 102:110504, Mar 2009.

[90] Y. Zhang et al. Long-distance continuous-variable quantum key distribution over 202.81 km of fiber. *Phys. Rev. Lett.*, 125:010502, Jun 2020.

[91] W. Wiesbeck, L. Sit, M. Younis, G. Krieger, and A. Moreira. Radar 2020: The future of radar systems. 07 2015.

[92] X. Wang, H. Z. Pan, K. Guo, X. Yang, and S. Luo. The evolution of LiDAR and its application in high precision measurement. *IOP Conference Series: Earth and Environmental Science*, 502:012008, jun 2020.

[93] A. Moreira. Spaceborne radar technologies for earth remote sensing. pages 33–36, 09 2007.

[94] H. Klinkrad. Monitoring space – efforts made by european countries. https://fas.org/spp/military/program/track/klinkrad.pdf.

[95] J.-Q. Xi et al. Optical thin-film materials with low refractive index for broadband elimination of fresnel reflection. *Nature Photonics*, 1(3):176–179, Mar 2007.

[96] C. Campbell. Fresnel Diffraction Of Gaussian Laser Beams By Circular Apertures. *Optical Engineering*, 26(3):270 – 275, 1987.

[97] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters. Purification of noisy entanglement and faithful teleportation via noisy channels. *Phys. Rev. Lett.*, 76:722–725, Jan 1996.

[98] L. Jiang, J. M. Taylor, K. Nemoto, W. J. Munro, R. Van Meter, and M. D. Lukin. Quantum repeater with encoding. *Phys. Rev. A*, 79:032325, Mar 2009.

[99] L.-M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller. Long-distance quantum communication with atomic ensembles and linear optics. *Nature*, 414(6862):413–418, Nov 2001.

[100] C. T. Nguyen et al. Quantum network nodes based on diamond qubits with an efficient nanophotonic interface. *Phys. Rev. Lett.*, 123:183602, Oct 2019.

[101] S. Abruzzo et al. Quantum repeaters and quantum key distribution: Analysis of secret-key rates. *Phys. Rev. A*, 87:052315, May 2013.

[102] N. Sangouard, C. Simon, H. de Riedmatten, and N. Gisin. Quantum repeaters based on atomic ensembles and linear optics. *Rev. Mod. Phys.*, 83(1):33–80, Mar 2011.

[103] L. Jiang, J. M. Taylor, and M. D. Lukin. Fast and robust approach to long-distance quantum communication with atomic ensembles. *Phys. Rev. A*, 76:012301, Jul 2007.

[104] A. M. Stephens, J. Huang, K. Nemoto, and W. J. Munro. Hybrid-system approach to fault-tolerant quantum communication. *Phys. Rev. A*, 87:052333, May 2013.

[105] S. Muralidharan, J. Kim, N. Lütkenhaus, M. D. Lukin, and L. Jiang. Ultrafast and fault-tolerant quantum communication across long distances. *Phys. Rev. Lett.*, 112:250501, Jun 2014.

[106] D. P. DiVincenzo. The physical implementation of quantum computation. *Fortschritte der Physik*, 48(9□11):771–783, 2000.

[107] K. Azuma, K. Tamaki, and H.-K. Lo. All-photonic quantum repeaters. *Nature Communications*, 6:6787 EP –, Apr 2015.

[108] K. Boone et al. Entanglement over global distances via quantum repeaters with satellite links. *Phys. Rev. A*, 91:052325, May 2015.

[109] S. Khatri, A. J. Brady, R. A. Desporte, M. P. Bart, and J. P. Dowling. Spooky action at a global distance: analysis of space-based entanglement distribution for the quantum internet. *npj Quantum Information*, 7(1):4, Jan 2021.

[110] H. de Riedmatten, M. Afzelius, M. U. Staudt, C. Simon, and N. Gisin. A solid-state light-matter interface at the single-photon level. *Nature*, 456(7223):773–777, 2008.

[111] M. Afzelius, C. Simon, H. de Riedmatten, and N. Gisin. Multimode quantum memory based on atomic frequency combs. *Phys. Rev. A*, 79:052329, May 2009.

[112] M. Gündoğan et al. Space-borne quantum memories for global quantum communication. *arXiv*, 2006.10636, 2020.

[113] M. K. Bhaskar et al. Experimental demonstration of memory-enhanced quantum communication, 2019.

[114] N. K. Bernardes, L. Praxmeyer, and P. van Loock. Rate analysis for a hybrid quantum repeater. *Phys. Rev. A*, 83:012323, Jan 2011.

[115] T. Vergoossen, S. Loarte, R. Bedington, H. Kuiper, and A. Ling. Modelling of satellite constellations for trusted node qkd networks. *Acta Astronautica*, 173:164–171, 2020.

[116] L. Mazzarella et al. Quarc: Quantum research cubesat—a constellation for quantum communication. *Cryptography*, 4(1), 2020.

[117] N. Vyas and R. Alleaume. Everlasting secure key agreement with performance beyond qkd in a quantum computational hybrid security model. *arXiv*, 2004.10173, 2020.

Paper 1

The material in this chapter has been reproduced from the following publication [17]:

Carlo Liorni, Hermann Kampermann and Dagmar Bruß, Satellite-based links for quantum key distribution: beam effects and weather dependence, *New J. Phys.* 21 093055, 2019

Satellite-based links for Quantum Key Distribution: beam effects and weather dependence

Carlo Liorni[1], **Hermann Kampermann**[1], **Dagmar Bruß**[1]

[1]Heinrich Heine Universität, Institut für Theoretische Physik III, Universitätsstraße 1, 40235, Düsseldorf, Germany.

Abstract. The establishment of a world-wide quantum communication network relies on the synergistic integration of satellite-based links and fiber-based networks. The first are helpful for long-distance communication, as the photon losses introduced by the optical fibers are too detrimental for lengths greater than about 200 km. This work aims at giving, on the one hand, a comprehensive and fundamental model for the losses suffered by the quantum signals during the propagation along an atmospheric free-space link. On the other hand, a performance analysis of different Quantum Key Distribution (QKD) implementations is performed, including finite-key effects, focusing on different interesting practical scenarios. The specific approach that we chose allows to precisely model the contribution due to different weather conditions, paving the way towards more accurate feasibility studies of satellite-based QKD missions.

Keywords: Satellite links, Quantum Key Distribution, Atmospheric effects

1. Introduction

Quantum Key Distribution (QKD) and Quantum Communications in general have the potential to revolutionise the way we communicate confidential information over the internet. The natural carriers for quantum information are photons, that are already widely used in classical networks of optical fibers to achieve high communication rates. Unfortunately, even though enormous improvements have been obtained in the last years [1, 2], scaling quantum communication protocols over long distances is very challenging, due to the losses experienced during the propagation inside the optical fibers. Several schemes for the realization of quantum repeaters have been proposed in recent years, that could allow to bridge long distances and naturally be implemented inside a quantum communication network [3, 4, 5, 6, 7]. Considering the important technological hurdles that quantum repeaters should overcome before becoming useful, satellite-based free-space links look like the most practical way to achieve long-distance QKD in the short term [8]. They can take advantage of the satellite technology and the optical communication methods developed in the last decades in the classical case. Various feasibility studies had addressed this topic in the last twenty years [9, 10, 8, 11] and several experiments have definitely proved that the technology involved is ready for deployment [12, 13, 14, 15, 16].

Optical satellite-based links have the important drawback of being strongly dependent on the weather conditions [17, 18, 19, 20]. The presence of turbulent eddies and scattering particles like haze or fog generates random fluctuations of the relative permittivity of the air, on different length- and time-scales. This phenomenon affects the light propagation in a complicated way, inducing random deviations and deformations of any optical beam sent through the atmosphere. It results in reduced transmittance, because of geometrical losses due to the finite collection aperture, and random modifications of the phase front. A comprehensive model of these effects is then necessary, in order to precisely evaluate the performance of the link when used for quantum communication protocols.

In this work we generalize the approach proposed in [21, 22] to satellite-based links and we evaluate their losses in several practical cases, under different weather conditions. This information is then used to assess the performance of the link in terms of the achievable key rates using different implementations of QKD. The case of *Low Earth Orbit* (LEO) satellites is addressed, assuming different payloads and sizes of the optical elements.

This work is organized as follows. In Sec. 2 we introduce the problem of free-space optical links and an analytical method to study them. The discussion continues in Appendix A. In Sec. 3 a detailed description of the model used to simulate the satellite-based link is presented. Then, the main results are shown and discussed, together with pros and cons of our approach. In Sec. 4 we use the analysis of the transmittance of the channel conducted in the previous section to study the key rate achievable by different QKD implementations, in some interesting real-life scenarios. The analysis concerning

the use of smaller and more affordable satellites is performed in Sec. 5. Finally, the results are summarized and discussed in Sec. 6. The appendix starts with a recap of the results of [21, 22] (Appendix A) and their application to the problem at hand (Appendix B). Then two models for the estimation of the stray light satellite links [11, 23] are presented in Appendix C. Appendix D is devoted to the definition of the QKD protocols we use in Sec. 4 and the expression of the correspondent key rates. In Appendix E we report the parameters chosen for the simulations and we discuss their pertinence.

2. Free-space optical links and the Elliptic Beam Approximation

The problem that we address in the first part of the work is the following. A Gaussian beam is sent, either from an orbiting transmitter or from a ground station, through a non-uniform link partially inside the atmosphere and partially in vacuum. We are interested in the transmittance of the received beam through a circular aperture of radius a (the receiving telescope)

$$\eta = \int_{|\boldsymbol{\rho}|^2=a^2} d^2\boldsymbol{\rho}\ |u(\boldsymbol{\rho}, L)|^2\ , \tag{1}$$

which is a random variable, because of the intrinsic randomness of the fluctuations in the medium. Here $u(\boldsymbol{\rho}, L)$ is the beam envelope at the receiver plane (at distance L from the transmitter, with $\boldsymbol{\rho}$ the position in the transverse plane).

The so-called *Elliptic Beam Approximation* [21] greatly simplifies the analysis: the atmosphere is assumed to generate only

- deflection of the beam as a whole (*Beam Wandering*)
- elliptic deformations of the beam profile
- extinction losses due to back-scattering and absorption.

In this case the state of the beam at the receiver plane is completely described by the vector of parameters (refer to Fig 1)

$$\mathbf{v} = (x_0, y_0, W_1, W_2, \varphi_0)\ , \tag{2}$$

representing the beam-centroid coordinates, the principal semi-axes of the elliptic profile and the angle of orientation of the ellipse. The transmittance is then a function of these beam parameters and the radius of the receiving aperture.

The fluctuations of the relative permittivity of the atmospheric air can be statistically modeled [24, 25, 26, 27, 28, 29, 30, 31, 32]. The probability distribution of the parameters in Eq. (2) can then be analytically estimated, as shown in [21, 22]. A brief recap of the derivation and the main results is presented in Appendix A. This allows, through random sampling, to obtain the Probability Distribution of the Transmittance (PDT), an important figure of merit for fluctuating links. This approach gives no information about the phase of the wavefront, but this is not a problem when phase-insensitive measurements are considered (e.g., the BB-84 QKD protocol that we analyze in Sec. 4).

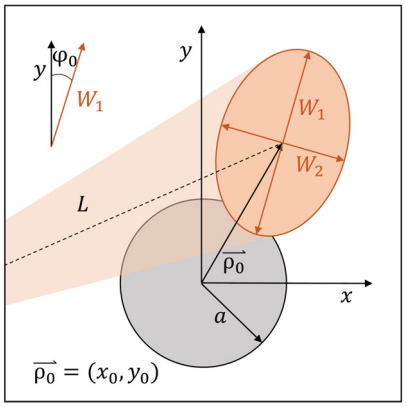

Figure 1. Schematic representation of the received beam and receiving aperture. L is the length along the propagation direction, a the radius of the receiving aperture, $\boldsymbol{\rho}_0 = (x_0, y_0)$ is the beam-centroid position, W_1 and W_2 the two axes of the elliptical profile, φ_0 the angle of orientation of the ellipse.

3. Satellite-based links: model and results

The atmosphere can in general be divided into several layers, depending on the properties of different physical parameters, like density of the air, pressure, temperature, density of ionized particles, and so on. This structure is site-dependent, especially regarding the thickness of the different layers. For this reason, in this work we assume a simplified version of a satellite-based optical link: a uniform atmosphere up to a certain altitude $\bar{h}$, then vacuum all the way up to the satellite (at altitude $\bar{L}$), as pictured in Fig.2. Instead of a continuum of values describing the physical quantities as a function of the altitude, we now have only two parameters, namely the value of the quantity inside the uniform atmosphere and the effective thickness $\bar{h}$. This is likely to be a good approximation, because the atmospheric effects are prominent only in the first 10 to 20 km from the ground, while usual orbit height for LEO satellites are above 400 km. For the remainder of the paper we choose a minimum altitude of the satellite $\bar{L} = 500$ km, achieved exactly above the ground station. In this case, the extension of the orbit of the satellite which can be usable for key distribution corresponds roughly to the interval $L \in [500, 2000]$ km, corresponding to angles from the zenith in the interval $[0, 80°]$. The effective thickness of the atmosphere $\bar{h}$ is fixed here to 20 km, for the considerations above.

As introduced in Sec.2, we want to generalize the model proposed in [21, 22] to the just described case of a non-uniform link between the ground and a satellite. The computation follows the same steps and is described in Appendix A and Appendix B. First of all we need to evaluate Eqs. (A.13), (A.14) and (A.15) in order to compute the moments of the distributions of the elliptic beam parameters (Eq. (2)). To do so, an integration along the propagation path must be performed (Eqs. (A.19) and (A.20)). Here we introduce the considerations of the previous paragraph, imposing that the parameters measuring the strength of the atmospheric effects are constant (greater

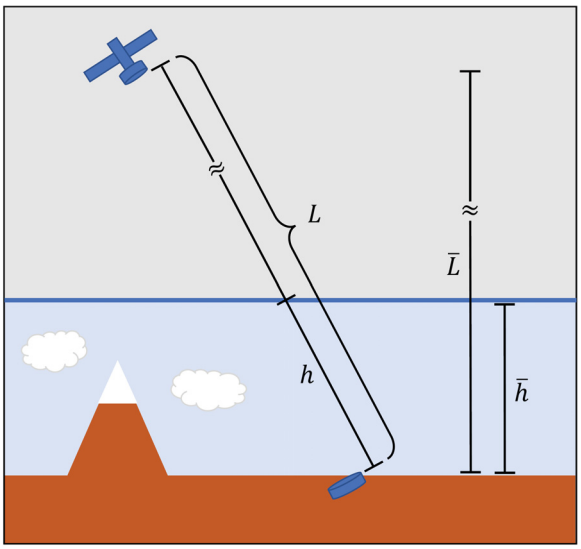

Figure 2. The non-uniform free-space link between the satellite and the ground station is depicted here (not in scale). The main parameters shown are the thickness of the atmosphere $\bar{h}$, the height of the satellite $\bar{L}$, the total distance between sender and receiver L and the length of the propagation inside the atmosphere h.

than 0) inside the atmosphere and 0 outside. In particular we assume

$$\begin{aligned} \text{Down} - \text{links} \qquad & C_n^2(z) = C_n^2\ \Theta(z-(L-h)) \\ & n_0(z) = n_0\ \Theta(z-(L-h)) \\ \text{Up} - \text{links} \qquad & C_n^2(z) = C_n^2\ \Theta(h-z) \\ & n_0(z) = n_0\ \Theta(h-z)\ , \end{aligned} \tag{3}$$

where C_n^2 is the value of the refractive index structure constant and n_0 is the density of scattering particles. $\Theta(z)$ is the so-called Heaviside step-function, z is the longitudinal coordinate, L is the total length of the link and h is the length traveled inside the atmosphere, as shown in Fig. 2. A down-link corresponds to the situation of satellite-to-ground communication, so the atmospheric effects kick-in only for $z > (L-h)$ (final section of the propagation), while for up-links it is limited to $z < h$. We remark that some models for the altitude-dependence of the optical quantities, like C_n^2, are available in the literature [33, 34, 35, 36, 37], but they are correct only in the geographical site and in the atmospheric conditions in which they had been experimentally extracted (more details in Appendix E). Additional extinction losses due to back-scattering and absorption in the atmosphere are modeled by a parameter χ_{ext}, as described in Appendix A. Its value is adjusted from the analysis performed in [10] based on the MODTRAN5 software [38]. In this model, the values of C_n^2 and n_0 completely describe the atmospheric conditions together with the thickness $\bar{h}$ and the extinction factor χ_{ext}.

Following the analysis of Appendix A (in particular equations Eq. (A.13), (A.14), (A.15)), we compute the first and second moments of the beam parameters in Eq. (2) for the link described in Eq. (3). The distribution of the angle of orientation of the

elliptical profile φ_0 is assumed uniform in $[0, \pi/2]$ as in [21, 22]. The mean value and variance of the beam centroid position are the same for x and y directions and equal to (Eq. (A.13))

$$\langle x_0 \rangle = \langle y_0 \rangle = 0 \ , \qquad \langle x_0^2 \rangle = \langle y_0^2 \rangle = 0.419 \ \sigma_R^2 \ W_0^2 \ \Omega^{-\frac{7}{6}} \frac{h}{L} \ , \tag{4}$$

where the quantity $\sigma_R^2 = 1.23 \ C_n^2 \ k^{\frac{7}{6}} L^{\frac{11}{6}}$ is the so-called Rytov parameter and $\Omega = \frac{kW_0^2}{2L}$ is the Fresnel number. The condition $\langle x_0 \rangle = 0$ is achieved by proper pointing. The first two moments of the semi-axes of the ellipse squared, W_i^2 with $i = 1, 2$, are instead estimated from Eq. (A.14) and (A.15)

$$\langle W_i^2 \rangle = \frac{W_0^2}{\Omega^2} \Big(1 + \frac{\pi}{8} \ L \ n_0 \ W_0^2 \frac{h}{L} + 2.6 \ \sigma_R^2 \ \Omega^{\frac{5}{6}} \frac{h}{L} \Big) \tag{5}$$

$$\langle \Delta W_i^2 \Delta W_j^2 \rangle = (2\delta_{ij} - 0.8) \ \frac{W_0^4}{\Omega^{\frac{19}{6}}} \Big(1 + \frac{\pi}{8} \ L \ n_0 \ W_0^2 \frac{h}{L} \Big) \sigma_R^2 \frac{h}{L} \ . \tag{6}$$

Similar expressions hold for down-links, for the beam centroid position

$$\langle x_0 \rangle = \langle y_0 \rangle = 0 \qquad \langle x_0^2 \rangle = \langle y_0^2 \rangle = \alpha \ L \tag{7}$$

and for the semi-axes of the elliptical profile

$$\langle W_i^2 \rangle = \frac{W_0^2}{\Omega^2} \Big(1 + \frac{\pi}{24} \ L \ n_0 \ W_0^2 \Big(\frac{h}{L} \Big)^3 + 1.6 \ \sigma_R^2 \ \Omega^{\frac{5}{6}} \Big(\frac{h}{L} \Big)^{\frac{8}{3}} \Big) \tag{8}$$

$$\langle \Delta W_i^2 \Delta W_j^2 \rangle = (2\delta_{ij} - 0.8) \frac{3}{8} \frac{W_0^4}{\Omega^{\frac{19}{6}}} \Big(1 + \frac{\pi}{24} \ L \ n_0 \ W_0^2 \Big(\frac{h}{L} \Big)^3 \Big) \sigma_R^2 \Big(\frac{h}{L} \Big)^{\frac{8}{3}} \ , \tag{9}$$

where $\alpha \sim 2 \ \mu$rad is the angular pointing error.

There are two main differences between the expressions related to the up-link and down-link configurations. First, they depend on a different power of the ratio $\frac{h}{L}$. As $\frac{h}{L} \ll 1$, we deduce, as expected, that the atmospheric effects are much stronger for up-links than for down-links. The phenomena involved here (beam deflection and broadening) are angular effects, whose contribution on the final size of the beam (and thus, on the losses of the channel) are proportional to the distance traveled after the "kick in" of the effect. For up-links, these effects happen very close to the transmitter, and then the beam broadens for hundreds of km before being detected. In the down-link scenario, instead, the beam travels in vacuum for the largest portion of the distance, and the atmospheric effects take place only at the end of the propagation, in the last tens of km before the receiver. The second difference resides in the origin of the fluctuations of the beam centroid position x_0. For up-links, in fact, the deflections induced by the atmospheric effects are usually much stronger than the pointing error, which we neglect. For down-links, instead, at the top of the atmosphere the beam dimensions are already much larger than any turbulent inhomogeneity. In this case the induced beam wandering can be neglected and the pointing error becomes the main contribution.

The knowledge of the probability distribution of the elliptic beam parameters is then used to compute the PDT, through Eq. (A.22) and random sampling. Two

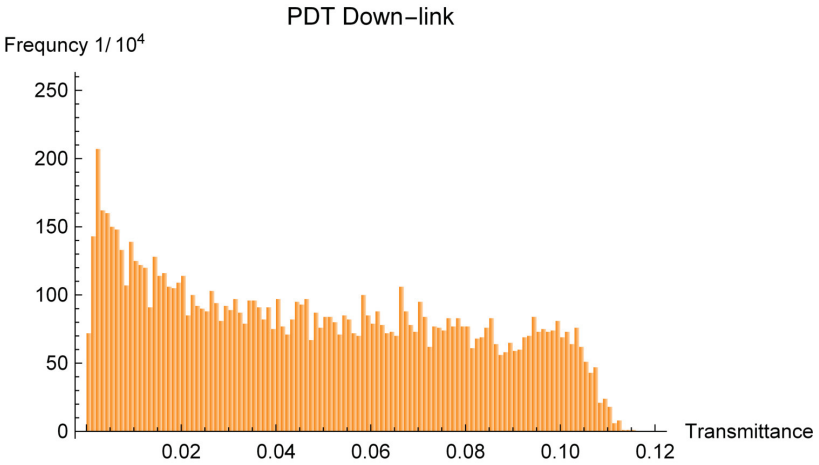

Figure 3. The Probability Distribution of the Transmittance (PDT) $\mathcal{P}(\eta)$ reconstructed by means of the method presented in Sec.3 and Appendix A. The situation under study is a down-link at high elevation angles ($L = 500$ km) and the histogram has been obtained on the basis of 10000 events. The parameters of the setup are reported in Appendix E.

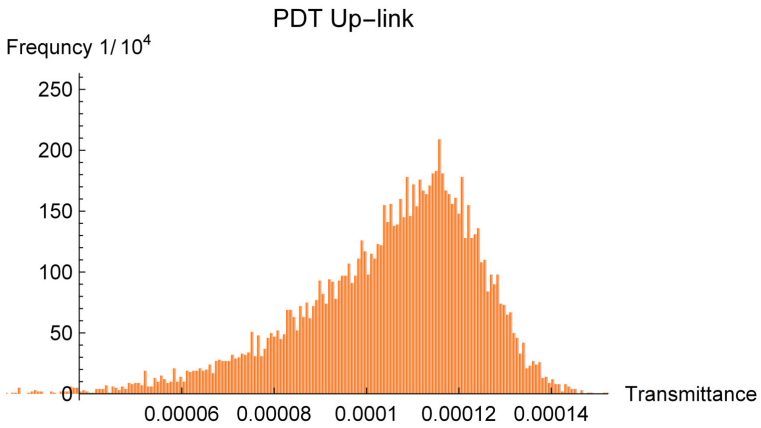

Figure 4. The Probability Distribution of the Transmittance (PDT) $\mathcal{P}(\eta)$ reconstructed by means of the method presented in Sec.3 and Appendix A. The situation under study is an up-link at high elevation angles ($L = 500$ km) and the histogram has been obtained on the basis of 10000 events. The parameters of the setup are reported in Appendix E.

examples are shown in Fig. 3 and Fig. 4 for a down-link and an up-link, respectively. The considerations of the previous paragraph can naturally be used to explain the difference in the shape of these two distributions. For down-links, especially at high elevation angles, like the case shown in Fig. 3, the value of the beam width at the receiver is comparable to the wandering induced by pointing errors. This means that it can happen that the beam wanders completely off the receiving aperture, giving values of transmittance close to 0. In the up-link case, instead, the beam broadening gets the upper hand: the beam at the receiver is so large that the wandering induced by the

atmosphere cannot change the total transmittance very much. It results in a rather narrow distribution, peaked at much lower values of transmittance with respect to the down-link case.

Now we want to study the expected loss introduced by the link as a function of the total link length. We show in figures 5 and 6 the mean value of the PDT as a function of the angle from the zenith and the total link length, for down-links and up-links, under different weather conditions. Every point in the graph has been obtained, just like in Fig. 3 and Fig. 4, from 1000 samples of the parameters in Eq. (2) and using Eq. (A.22). The asymmetric nature of the PDT for some configurations of the link can make the use of the mean value partially misleading, however, the full PDT will be used in the next section to compute the secret key rates.

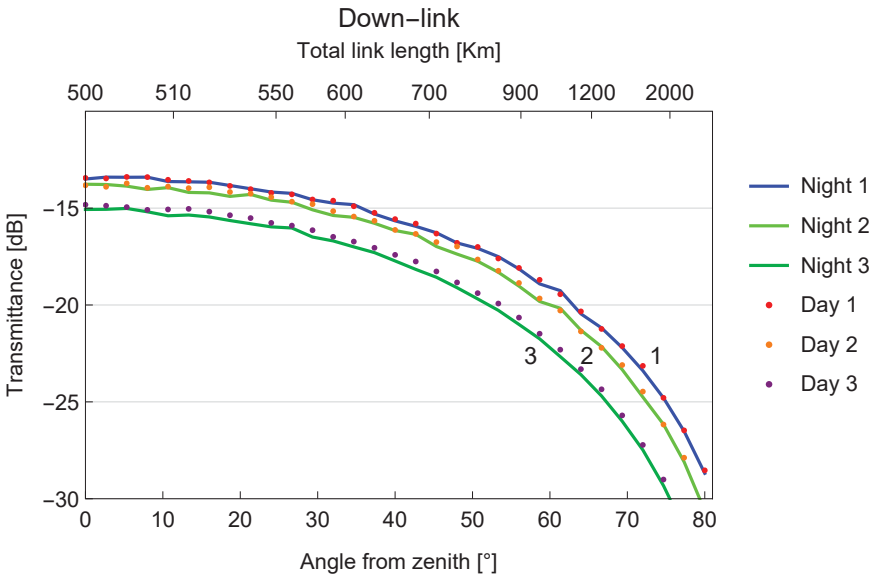

Figure 5. Mean value of the Probability Distribution of the Transmittance (PDT) as a function of the zenith angle and total link length for the down-link configuration, under various weather conditions during night- and day-time. Situation 3 corresponds to worse weather conditions with respect to 2, that is in turn worse than 1. From a quantitative point of view, this means that the values of the parameters C_n^2 and n_0 grow going from 1 to 3. See Tab. E2 in Appendix E for details about the choice of the parameters. From a qualitative point of view, they correspond to clear, slightly foggy and moderately foggy nights (Night 1-2-3) and to not windy, moderately windy and windy day (Day 1-2-3). Note that worse weather conditions generally correspond to higher extinction in the atmosphere. However, in order to highlight the contribution of the beam effects (broadening, wandering and shape distortion), we kept the value of χ_{ext} fixed in this analysis, as well as in figure 6. The non-uniformities are due to the finite statistics, every point corresponds to 1000 samples.

The critical parameters here are, apart from the ones related to the atmospheric effects, the diameter of the sending and receiving telescopes and the signal wavelength. We chose $D_{\text{sat}} = 30$ cm for the orbiting one, $D_{\text{grnd}} = 1$ m for the ground station telescope and $\lambda = 800$nm. These are demanding values, consistent with the Chinese

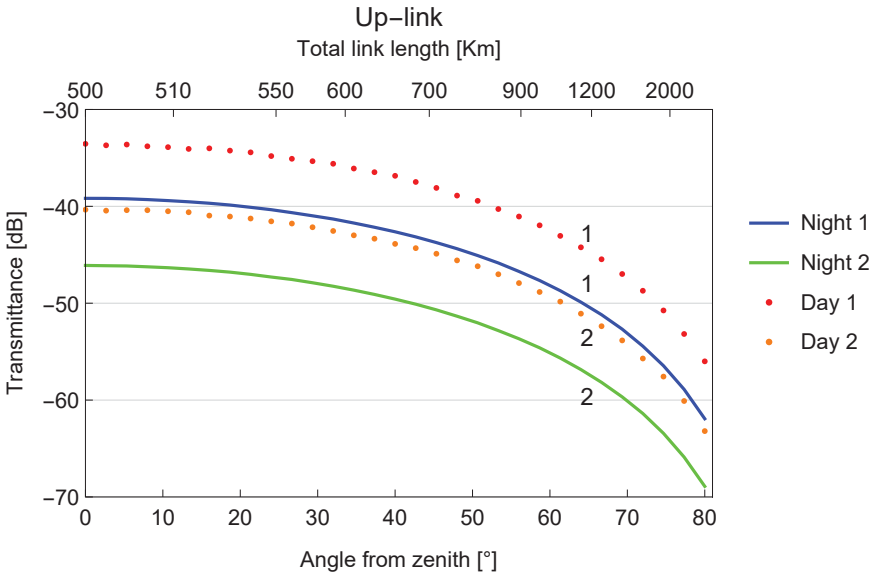

Figure 6. Mean value of the Probability Distribution of the Transmittance (PDT) as a function of the zenith angle and total link length for the up-link configuration, under various weather conditions during night- and day-time. Same considerations as Fig. 5 apply.

mission *Micius* (see [12, 13, 14, 15] for details). Further analysis are reported in Sec.5. We notice here that the assumption of perfect Gaussian beams sent by the transmitter is not very realistic. Standard telescopes generate beams with intensity distributions rather close to a circular Gaussian profile but with some imperfections, introduced for example by the truncation at the border of the optical elements. The main downside is that such beams will exhibit larger intrinsic beam broadening due to diffraction. In our model this effect can be taken into account by adjusting the value of the initial beam waist W_0, in order to match the far-field divergence expected from the imperfect quasi-Gaussian beam.

Our analysis confirms that, at least for the parameters chosen for the simulation, down-links are much preferable over up-links for quantum communication due to the smaller losses. However, up-links can still achieve losses below the threshold for the accomplishment of quantum communication tasks, QKD included. Particularly interesting is the comparison between night- and day-time operation. During the day, the higher temperatures bring stronger wind and more active mixing between the different layers of the atmosphere, leading to more pronounced turbulence effects. However, on average, during clear days the moisture content of the lower atmosphere is smaller than at night, resulting in weaker beam spreading due to scattering particles. At night, instead, the lower temperature results, on one hand, in a less turbulent atmosphere and, on the other, in the formation of haze and mist. In this situation, the contribution of scattering over such particulate can be stronger than the turbulence-induced effects.

We point out that in this analysis the path elongation due to refraction in the atmosphere has not been taken into account, as it gives substantial effects only at low

elevation angles ($\leq$ 10°). This and other zenith-angle-dependent effects have been thoroughly studied in [39].

Many different models for atmospheric channels and satellite-based links had already been proposed in the literature, due to the increasing interest in free-space optical communication. A comparison with them can highlight the strengths of the approach we reported in this section. Many feasibility studies [40] rely on models that average the intensity over sufficiently long times, so that the only atmospheric effect is overall a broadening of the beam. This approach gives no information on the PDT of the channel, that can be useful in many instances (for example, to apply post-selection techniques). A different approach has been chosen by [10], based on convolution between the beam envelope and the time-averaged pointing errors and beam broadening, leading again to no information about the PDT. A popular technique, that involves heavy numerical computations, is based on simulating the effect of the atmosphere by random phase screens regularly distributed along the propagation path in vacuum [41, 42, 43]. Many theoretical works have been devoted to find the analytical probability distribution that better fits the experimentally measured transmittance of free-space optical links. Mainly used are the log-normal [44, 45], Gamma-Gamma [46] and Double Weibull [47] distributions. Each of them appears to be more suitable depending on the strength of the turbulence, the length of the link and the configuration of the transmitting and receiving telescopes. On the contrary, the approach used here is a constructive method that allows to determine the PDT starting from the characteristics of the beam and the atmospheric conditions.

It has been shown that a post-selection of the time-intervals with greater transmittance can help to increase the secret key rates [48, 49, 50]: in this context, the ability of our approach to simulate not only the expected value of the transmittance, but its probability distribution too, may prove to be of great interest. In [51] the authors showed that the detrimental effects of asymmetric and fluctuating losses in Measurement-Device-Independent (MDI) QKD with decoy states can be counteracted by means of additional losses introduced by the central node. In this context, when the quantum links used are free-space, the information about the PDT allows to optimize such compensation losses to maximize the key rate.

Finally, we effectively take into account the contribution due to scattering particles, like fog or haze, making possible to model the effect of different weather conditions, a problem usually not addressed in previous works. It is particularly important during night-time operation, where a substantial amount of beam deformations can be imputed to scattering on moisture particles.

4. Performance of QKD implementations

The transmittance shown in Fig. 5 and 6 can now be used to compute the expected secret key rates of a QKD protocol. In the following we analyze the performance of the BB-84 protocol [52] with polarization encoding, implemented using either a true Single Photon

(SP) source or Weak Coherent Pulses (WCPs). We use modern techniques to compute the secret key rates for SPs [53] and WCPs with decoy states [54, 55, 56, 57], taking into account finite-key effects. The key rates are averaged over the PDT computed for different link lengths and configurations

$$\bar{R} = \int_0^1 R(\eta)\ \mathcal{P}(\eta)\ d\eta = \sum_{i=1}^{N_{\text{bins}}} R(\eta_i)\ \mathcal{P}(\eta_i)\ . \tag{10}$$

Here $\bar{R}$ is the averaged key rate, $R(\eta)$ the key rate at the specific value of the transmittance, $\mathcal{P}(\eta)$ is the PDT. The integral average is approximated dividing the range $[0, 1]$ in N_{bins} bins, centered in η_i for $i = 1,\ N_{\text{bins}}$, and taking the weighted sum of the rates. $\mathcal{P}(\eta_i)$ is estimated through random sampling, as pointed out in Sec. 3. The expressions for the key rates $R(\eta)$ for the different implementations are given in Appendix D, see Eq. (D.1) for SPs and Eq. (D.2) for WCPs.

The biggest source of noise in free-space optical links is represented by environmental light entering in the receiver telescope together with the signal photons. Simple models to estimate the amount of stray light [11, 23] are given in Appendix C for down-links and up-links. In the following analysis we consider the number of stray photons to be independent of the position of the satellite. Particular situations concerning light pollution, like the presence of a city close to the ground station, may require a more specific model for low elevation angles.

The secret key rate resulting from a down-link and an up-link are reported in Fig. 7 and Fig. 8, for both night-time and day-time operation, under good weather conditions, corresponding to situation 1 in Fig. 5. We also report in the graphs the correspondent Quantum Bit Error Rate (QBER), defined in Eq. C.4 in Appendix C, averaged over the PDT. In the following we set the block sizes at 10^6 for SPs and at 10^8 for WCPs in down-link. This difference is justified by the higher repetition rates obtainable by modern WCP sources with respect to (still under development) true SP sources. Consider that the total link duration is around 300 s, corresponding to the complete passage of a LEO satellite over the ground station. In this time span, assuming a repetition rate of 10 MHz for SP sources and 1 GHz for WCP sources, several blocks of the size specified above can be exchanged in the down-link configuration. Due to the higher losses encountered in an up-link, the block size is lowered to 10^5 for SPs and at 10^7 for WCPs.

At night it is possible to establish a non-zero key rate in down-link during the whole passage of the satellite in the SP implementation. Using WCPs, instead, the key rate drops to 0 when the satellite is around 20° over the horizon. In the daytime, instead, due to the stronger background light, the key rate vanishes at higher elevation angles, even considering improved spatial, spectral and temporal filtering. According to [23], the typical brightness of the sky background (see also Sec. Appendix C) in a clear day is about 3 orders of magnitude higher than during a full-moon night. We found that, in order to achieve a non-zero key rate for a reasonable portion of the transit, the filtering of the stray light must be tighter than during the night of a factor $\gtrsim 100$, obtained

acting on the field of view of the telescope and the width of the spectral filters (refer to Tab. E3 in Appendix E for details).

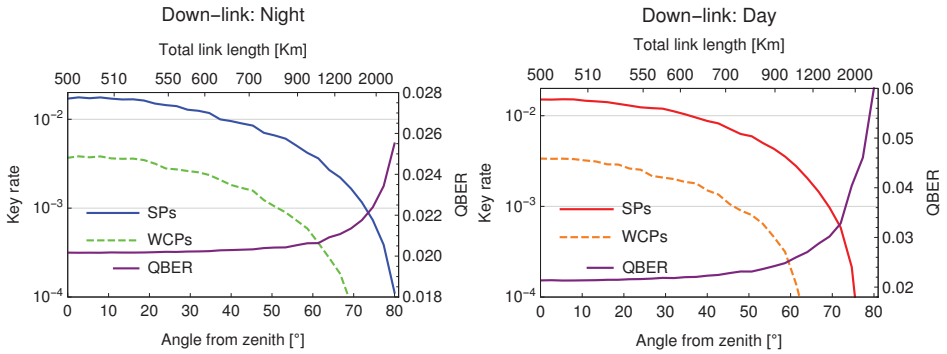

Figure 7. The key rate generated by the BB-84 protocol with SP and WCP implementations is reported as a function of the zenith angle and the total link length, for a down-link, together with the QBER. We assume here good weather conditions, corresponding to situation 1 in Fig. 5.

Up-links have poorer performance due to higher losses, but we are still able to distill a secret key with non-zero rates during the night, with slightly improved filtering (Tab. E3 in Appendix E). The SP implementation reaches almost the same range (in elevation angle) as the down-link configuration, while the difference with WCPs is greater because of the smaller block size. For day-time operation the stronger background light makes the quantum bit error rate too high and the key rate vanishes, therefore we omit the corresponding graph. We stress that here (we refer to Appendix C for details) we did not consider artificial light pollution. So these results reliably simulate only ground stations which are isolated and far from big cities.

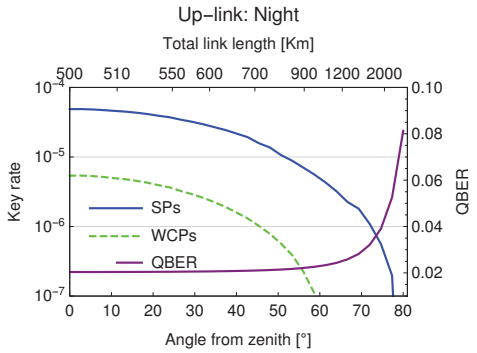

Figure 8. The key rate generated by the BB-84 protocol with SP and WCP implementations is reported as a function of the zenith angle and the total link length, for an up-link, together with the QBER. We assume here good weather conditions, corresponding to situation 1 in Fig. 5.

Note that the finite key effects can be very detrimental when the number of exchanged signals becomes too small. Particular attention must be payed when up-links are considered. In order to reproduce the results reported in Fig. 8, the block

length used in the security analysis is of the same order of magnitude of the number of signals exchanged during the whole passage of the satellite. This means that all the signals exchanged in a QKD session are processed in a single block in this case.

5. Cube-sat performance analysis

The simulations reported in Sec. 3 and Sec. 4 assume a quite demanding value of the optical aperture of the orbiting telescope. It is compatible with the *Micius* satellite [12, 13, 14, 15], operated by the *Chinese Academy of Science*, as part of the *Quantum Experiments at Space Scale* (QUESS) research project. The complexity and high cost of the mission make the use of such big satellites unfeasible for the establishment of a world-wide quantum communication network. Many recent proposals foresee the use of nano-satellites (e.g., *CubeSats* [58, 59, 60]) for QKD implementation [9, 61, 62, 63, 64]. The possibility to deploy many of such satellites in a single mission, to share the vector with other payloads and the modular nature lowers considerably the launch and building cost of these devices. They are usually loaded with smaller optics, of diameter ≤ 10 cm, even if larger apertures can be achieved with the use of deployable optics or bigger CubeSats (like the 12-Units satellite proposed in [63]). When used as transmitter, in the down-link configuration, the smaller aperture creates beams with much higher intrinsic divergence than the case studied in Sec. 3. In the up-link configuration, instead, smaller transmittance is due to the smaller collecting area. We show in Fig. 9 the results of the link simulation for down-links and up-links, in good weather conditions.

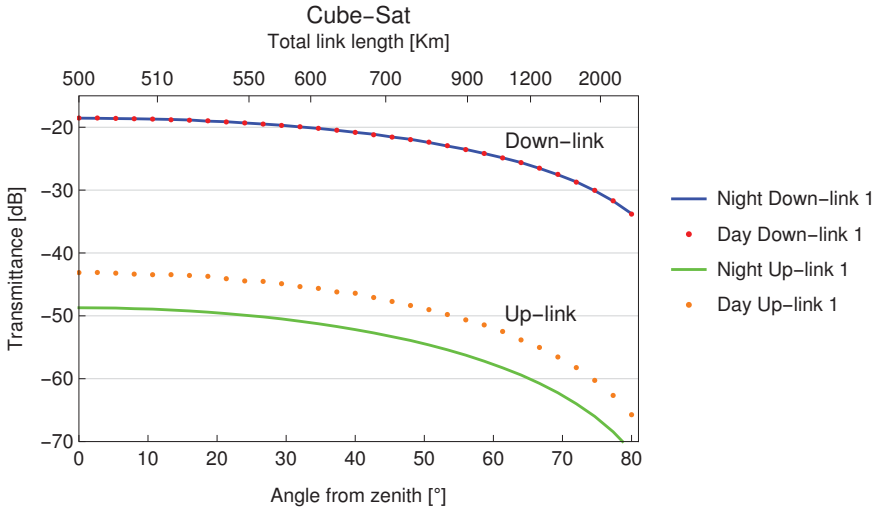

Figure 9. Mean value of the Probability Distribution of the Transmittance (PDT) as a function of the zenith angle and total link length for up-link and down-link configurations, using a Cube-sat with a 10 cm telescope. The weather conditions correspond to situation 1 in Fig. 5 and Fig. 6.

We see that the effect of the smaller optics diameter amounts to a difference in transmittance of about 5 dB for down-link and to 10 dB for up-links. Even though this

result favors the down-link configuration even more, we have to take into account that a smaller aperture will collect not only less signal light, but also less stray light. The resulting QBER for up-links, then, will be almost independent of the diameter of the receiving telescope (compare Fig. 8 and Fig. 11), if other parameters, such as the Field of View (FOV) of the telescope, are kept fixed (see Eq. C.1 in Appendix C for details).

The key rates achievable for nano-satellites in the down-link and up-link configurations are reported in Fig. 10 and Fig. 11. As expected, the range of angles over which a non-zero key rate can be exchanged shrinks with respect to the case of Sec. 4. We point out that we kept the block length fixed at the values reported in 4 even if, especially in the up-link configuration, that number of signals can't be exchanged in a single transit of the Cube-sat.

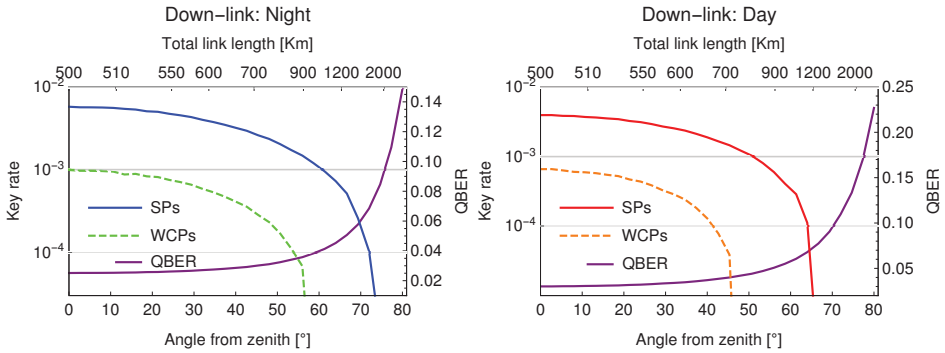

Figure 10. The key rate generated by the BB-84 protocol with SP and WCP implementations is reported as a function of the zenith angle and the total link length, for a down-link using a Cube-Sat, together with the QBER. We assume here good weather conditions, corresponding to situation 1 in Fig. 5

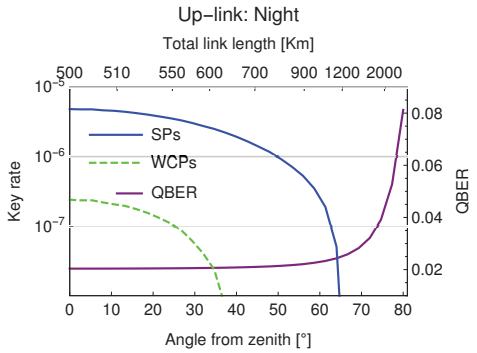

Figure 11. The key rate generated by the BB-84 protocol with SP and WCP implementations is reported as a function of the zenith angle and the total link length, for an up-link using a Cube-Sat, together with the QBER. We assume here good weather conditions, corresponding to situation 1 in Fig. 5

6. Conclusion

We provide a general and fundamental model to simulate the losses introduced by a satellite-based optical link, useful for feasibility and performance analysis of future free-space QKD experiments. The ability to precisely evaluate the contribution due to different weather conditions will be crucial in many situations. The geographical sites with better conditions can be more precisely mapped, in order to optimize the structure of future global quantum networks [65, 66, 67, 68, 69]. Through the use of this model, the data from meteorological predictions can directly be linked to the key rate achievable by the QKD link, allowing more accurate statistical studies of the number of operative days per year. The characterization of the transmittance of the channel has then be used to evaluate the performance of the link in terms of achievable secret key rates. We focused on two implementations of the BB-84 cryptographic protocol, using single photons and weak coherent pulses. The noise expected in interesting real-life scenarios, during night-time and day-time, has been modeled and taken into account. We also pointed out the importance of finite-key effects, which can be very detrimental due to the short duration of the link between ground station and satellite. The simulations confirm that long-distance quantum communications can be achieved not only using medium-sized satellites, like the Chinese *Micius*, but also nano-satellites, allowing to considerably cut the cost of a space-based global quantum network. Ultimately, such links are expected to be integrated with a repeater-based quantum network on the ground, to complement it and enhance the key rate when long distances need to be bridged. The analysis of such a configuration and the optimization of its topology and structure are still under study and represent a crucial milestone towards the realization of the dreamt quantum internet.

Acknowledgments

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No. 675662.

Appendix A. Free-space links with turbulence and scatterers

In this section we summarize the analysis of atmospheric optical channels proposed in [21, 22]. We will discuss the background, show the main steps of the derivation and recap some results, that will be used as starting point for the simulations described in Sec. 3.

We start from the introduction to the problem given in Sec. 1. The solution of the paraxial wave equation, with phase-approximation using the Huygens-Kirchhoff method [70], can be written in the following way

$$u(\boldsymbol{\rho}, L) = \int_{\mathbb{R}} d^2\boldsymbol{\rho}' u_0(\boldsymbol{\rho}') G_0(\boldsymbol{\rho}, \boldsymbol{\rho}'; L, 0) \times \exp[iS(\boldsymbol{\rho}, \boldsymbol{\rho}'; z, z')] \ . \tag{A.1}$$

Since the losses due to back-scattering and absorption can't be included in the paraxial approximation of the Helmholtz equation, we treat them phenomenologically multiplying the beam envelope $u(\boldsymbol{\rho}, L)$ by $\sqrt{\chi_{\rm ext}}$. The extinction factor $\chi_{\rm ext} \in [0, 1]$ accounts for absorption and back-scattering losses and can be considered as a non-fluctuating quantity (see [22]). In Eq. (A.1) $u_0(\boldsymbol{\rho}')$ is the Gaussian envelope at the transmitter plane ($z = 0$, z is the longitudinal coordinate)

$$u_0(\boldsymbol{\rho}) = \sqrt{\frac{2}{\pi W_0^2}} \exp\Big[- \frac{1}{W_0^2}|\boldsymbol{\rho}|^2 - \frac{ik}{2F}|\boldsymbol{\rho}|^2 \Big] \ , \tag{A.2}$$

with W_0 the beam spot radius at the transmitter, k the optical wavenumber and F the focal length of the beam. G_0 is a Gaussian integral kernel

$$G_0(\boldsymbol{\rho}, \boldsymbol{\rho}' : z, z') = \frac{k}{2\pi i (z - z')} \exp\Big[\frac{ik|\boldsymbol{\rho} - \boldsymbol{\rho}'|^2}{2(z - z')} \Big] \tag{A.3}$$

while S contains all the atmospheric effects

$$S(\boldsymbol{\rho}, \boldsymbol{\rho}'; z, z') = \frac{k}{2} \int_{z'}^{z} d\zeta \ \delta\varepsilon\Big(\boldsymbol{\rho} \frac{\zeta - z'}{z - z'} + \boldsymbol{\rho}' \frac{z - \zeta}{z - z'}, \zeta \Big) \ . \tag{A.4}$$

Here $S(\boldsymbol{\rho}, \boldsymbol{\rho}'; z, z')$ gives the phase contribution due to inhomogeneities of the relative permittivity of the air $\delta\epsilon(\boldsymbol{\rho}'', \xi)$ from z' to z. Note that $\delta\varepsilon$ can be separated in two contributions, related to turbulence and scattering

$$\delta\varepsilon = \delta\varepsilon_{\rm turb} + \delta\varepsilon_{\rm scat} \ . \tag{A.5}$$

Assuming the two contributions to be statistically independent, the same factorization holds for the permittivity fluctuation spectrum

$$\Phi_\varepsilon(\mathbf{K}) = \Phi_\varepsilon^{\rm turb}(\mathbf{K}) + \Phi_\varepsilon^{\rm scat}(\mathbf{K}) \ , \tag{A.6}$$

defined as the Fourier transform of the correlation function of $\delta\varepsilon(\mathbf{r})$

$$\langle \delta\varepsilon(\mathbf{r}_1) \delta\varepsilon(\mathbf{r}_2) \rangle = \int d^3\mathbf{K} \ \Phi_\varepsilon(\mathbf{K}) \exp[i\mathbf{K} \cdot (\mathbf{r}_1 - \mathbf{r}_2)] \ . \tag{A.7}$$

In the previous equations $\mathbf{K}$ denotes the momentum and is a 3-dimensional vector. The Markov approximation (that in our case corresponds to assume delta-correlation in the z direction) simplify this expression [25, 27]

$$\langle \delta\varepsilon(\mathbf{r}_1)\delta\varepsilon(\mathbf{r}_2)\rangle = 2\pi\delta(z_1 - z_2)\int d^2\mathbf{k}\ \Phi_\varepsilon(\mathbf{k})\ \exp[i\mathbf{k}\cdot(\boldsymbol{\rho}_1 - \boldsymbol{\rho}_2)] \tag{A.8}$$

where $\mathbf{k}$ represents the momentum in the plane transverse to the propagation direction. $\boldsymbol{\rho}_1$ and $\boldsymbol{\rho}_2$ are the components of the vectors $\mathbf{r}_1$ and $\mathbf{r}_2$ in the transversal plane, while $\delta(z)$ is the Dirac-delta. The Kolmogorov model allows us to write the turbulence-related part of the relative permittivity fluctuation spectrum as [24, 25, 26, 27]

$$\Phi_\varepsilon^{\text{turb}}(\mathbf{k}) = 0.132\ C_n^2\ |\mathbf{k}|^{-\frac{11}{3}}\ . \tag{A.9}$$

The refractive index structure constant C_n^2 characterizes the strength of turbulence in the optical domain and is an important parameter of the model. The scattering term in Eq. (A.6) can be approximated as a Gaussian function [28, 29, 30, 31, 32]

$$\Phi_\varepsilon^{\text{scat}}(\mathbf{k}) = \frac{n_0\zeta_0^4}{8\pi k^2}\ \exp[-\zeta_0^2|\mathbf{k}|^2]\ , \tag{A.10}$$

with ζ_0 correlation length of the fluctuations due to scattering particles. Here n_0 is the mean number of scatterers per unit volume and represents the main parameter in describing the strength of the scattering contribution.

Now we want to use these ingredients to calculate the probability distribution of the parameters in the elliptic beam approximation, introduced in Sec. 1

$$\mathbf{v} = (x_0, y_0, W_1, W_2, \varphi_0)\ . \tag{A.11}$$

First of all we define normalized variables from the ellipse semi-axes

$$\Theta_i = \ln\left(\frac{W_i^2}{W_0^2}\right) \quad i = 1, 2\ , \tag{A.12}$$

where W_0 is the beam spot radius at the transmitter. Now we assume that, in the case of uniform turbulence and scatterers density, the probability distribution of $x_0, y_0, \Theta_1, \Theta_2$ is Gaussian, while the angle of orientation φ_0 is uniformly distributed in $[0, \pi/2]$ (see Appendix of [22] for details). The mean value and the variance of these distributions can be analytically computed. We recall the main steps of the derivation in the following paragraphs.

Starting from the beam centroid position (x_0, y_0), we can choose the reference frame such that $\langle x_0\rangle = \langle y_0\rangle = 0$ and [25, 71]

$$\langle x_0^2\rangle = \langle y_0^2\rangle = \int_{\mathbb{R}^4} d^2\boldsymbol{\rho}_1 d^2\boldsymbol{\rho}_2 x_1 x_2 \Gamma_4(\boldsymbol{\rho}_1, \boldsymbol{\rho}_2; L)\ . \tag{A.13}$$

Here $\Gamma_4(\boldsymbol{\rho}_1, \boldsymbol{\rho}_2; z) = \langle u^*(\boldsymbol{\rho}_1, z)u(\boldsymbol{\rho}_1, z)u^*(\boldsymbol{\rho}_2, z)u(\boldsymbol{\rho}_1, z)\rangle$ is the fourth-order field correlation function.

The means and covariances of the squared ellipse semi-axes W_i^2 have the following form (see Appendix of [21] for details)

$$\langle W_{1/2}^2\rangle = 4\Big[\int_{\mathbb{R}^2} d^2\boldsymbol{\rho}\ x^2\ \Gamma_2(\boldsymbol{\rho}; L) - \langle x_0^2\rangle\Big]\ , \tag{A.14}$$

$$\langle \Delta W_i^2 \Delta W_j^2 \rangle = -8\Big\{ 2\Big(\int_{\mathbb{R}^2} d^2\boldsymbol{\rho}\ x^2\ \Gamma_2(\boldsymbol{\rho}; L)\Big)^2 - \int_{\mathbb{R}^4} d^2\boldsymbol{\rho}_1\ d^2\boldsymbol{\rho}_2\ [x_1^2 x_2^2(4\delta_{ij}-1) - x_1^2 y_2^2(4\delta_{ij}-3)] \times \Gamma_4(\boldsymbol{\rho}_1, \boldsymbol{\rho}_2; L)\Big\} - 16[4\delta_{ij}-1]\langle x_0^2\rangle^2\ , \tag{A.15}$$

where the second-order field correlation function $\Gamma_2(\boldsymbol{\rho}; z) = \langle u^*(\boldsymbol{\rho}, z) u(\boldsymbol{\rho}, z)\rangle$ has been used.

The next step is the calculation of the field correlation function, for which we use the expression of the beam envelope given in Eq. (A.1). We report the calculations only for $\Gamma_2(\boldsymbol{\rho}; L)$, the equivalent but more cumbersome expressions for $\Gamma_4(\boldsymbol{\rho}_1, \boldsymbol{\rho}_2; L)$ can be found in [22], Appendix B. Substituting Eq. (A.1) in the definition of $\Gamma_2(\boldsymbol{\rho}; z)$ yields

$$\Gamma_2(\boldsymbol{\rho}; L) = \int_{\mathbb{R}^4} d^2\ \boldsymbol{\rho}_1' d^2\boldsymbol{\rho}_2' u_0(\boldsymbol{\rho}_1') u_0^*(\boldsymbol{\rho}_2') G_0(\boldsymbol{\rho}, \boldsymbol{\rho}_1'; L, 0) \times G_0^*(\boldsymbol{\rho}, \boldsymbol{\rho}_2'; L, 0)\ \exp\Big[-\frac{1}{2}\mathcal{D}_S(0, \boldsymbol{\rho}_1' - \boldsymbol{\rho}_2')\Big]\ , \tag{A.16}$$

with the last term embodying the phase fluctuations due to the atmosphere (remember the definition of $S(\boldsymbol{\rho}, \boldsymbol{\rho}'; z, z')$ in Eq. (A.4))

$$\mathcal{D}_S(\boldsymbol{\rho}_k - \boldsymbol{\rho}_l, \boldsymbol{\rho}_k' - \boldsymbol{\rho}_l') = \Big\langle [S(\boldsymbol{\rho}_k, \boldsymbol{\rho}_k'; z, z') - S(\boldsymbol{\rho}_l, \boldsymbol{\rho}_l'; z, z')]^2 \Big\rangle\ . \tag{A.17}$$

Substituting Eq. (A.4) and exploiting again the Markov approximation, the factorization in Eq. (A.5) and (A.6) can be carried over

$$\mathcal{D}_S = \mathcal{D}_S^{\text{turb}} + \mathcal{D}_S^{\text{scat}}\ . \tag{A.18}$$

We can now introduce the models for the permittivity fluctuations spectrum related to turbulence (Eq. (A.9)) and scatterers (Eq. (A.10)), obtaining

$$\mathcal{D}_S^{\text{turb}}(\boldsymbol{\rho}, \boldsymbol{\rho}') = 2.95\ k^2\ L \int_0^1 d\xi\ C_n^2(\xi)\ |\boldsymbol{\rho}\xi + \boldsymbol{\rho}'(1-\xi)|^{\frac{5}{3}} \tag{A.19}$$

$$\mathcal{D}_S^{\text{scat}}(\boldsymbol{\rho}, \boldsymbol{\rho}') = \frac{\pi}{8} L \int_0^1 d\xi\ n_0(\xi)\ |\boldsymbol{\rho}\xi + \boldsymbol{\rho}'(1-\xi)|^2 \tag{A.20}$$

where we introduced the rescaled longitudinal coordinate $\xi \in [0, 1]$, where $\xi = 1$ corresponds to $z = L$. We allowed for a dependence on longitudinal coordinate in $C_n^2(\xi)$ and $n_0(\xi)$ for later use. We recall the definition of the so-called Rytov parameter $\sigma_R^2 = 1.23\ C_n^2\ k^{\frac{7}{6}} L^{\frac{11}{6}}$. Substituting in Eq. (A.16) the definition of the Gaussian envelope $u_0(\boldsymbol{\rho})$ (Eq. (A.2)) and the integral kernel $G_0(\boldsymbol{\rho}, \boldsymbol{\rho}' : L, 0)$ (Eq. (A.3)), the second-order field correlation function reads

$$\Gamma_2(\boldsymbol{\rho}; L) = \frac{\Omega^2}{\pi^2 W_0^4} \int_{\mathbb{R}^2} d^2\boldsymbol{\rho}'\ \mathrm{e}^{-\frac{\alpha}{2W_0^2}|\boldsymbol{\rho}'|^2 - 2i\frac{\Omega}{W_0^2}\boldsymbol{\rho}\cdot\boldsymbol{\rho}'} \exp\Big[-\frac{1}{2}\mathcal{D}_S^{turb}(0, \boldsymbol{\rho}')\Big] \exp\Big[-\frac{1}{2}\mathcal{D}_S^{scat}(0, \boldsymbol{\rho}')\Big]\ . \tag{A.21}$$

Here $\alpha = 1 + \Omega^2(1 - \frac{L}{F})^2$ with the Fresnel number defined as $\Omega = \frac{kW_0^2}{2L}$.

Integrating Eq. (A.21) (and the equivalent one for Γ_4) and then Eqs. (A.14), we obtain the first and second moments of the probability distribution of W_i^2. Then, the moments for the variables Θ_i are easily obtained from Eq. (A.12).

We consider now the transmittance, defined in Eq. (1), of an elliptic beam impinging on a circular aperture of radius a. It can be written as

$$\begin{aligned}\eta(x_0, y_0, W_1, W_2, \varphi_0) = \\ = \frac{2\ \chi_{\rm ext}}{\pi W_1 W_2} \int_0^a d\rho \int_0^{2\pi} d\theta\ \mathrm{e}^{-2A_1(\rho\ \cos\theta - \rho_0)^2} \\ \times\ \mathrm{e}^{-2A_2\rho^2 \sin^2\theta} \mathrm{e}^{-2A_3(\rho\ \cos\theta - \rho_0) r\ \ \sin\theta}\ ,\end{aligned} \tag{A.22}$$

with

$$\begin{aligned}A_1 &= \Big(\frac{\cos^2(\varphi_0 - \theta_0)}{W_1^2} + \frac{\sin^2(\varphi_0 - \theta_0)}{W_2^2}\Big) \\ A_2 &= \Big(\frac{\sin^2(\varphi_0 - \theta_0)}{W_1^2} + \frac{\cos^2(\varphi_0 - \theta_0)}{W_2^2}\Big) \\ A_3 &= \Big(\frac{1}{W_1^2} - \frac{1}{W_2^2}\Big)\ \sin\ 2(\varphi_0 - \theta_0)\ .\end{aligned} \tag{A.23}$$

In the previous equations (ρ, θ) are the integration variables in the area of the circular aperture, while $(x_0, y_0) = (\rho_0\ \cos\theta_0, \rho_0\ \sin\theta_0)$ is the beam-centroid position.

The Probability Distribution of the Transmittance (PDT) is then easily reconstructed. Extract at random M 5-tuples of values for $(x_0, y_0, \Theta_1, \Theta_2, \varphi_0)$, according to the correct probability distribution. Compute first the values of the ellipse semi-axes W_i from Θ_i and then the value of the transmittance for every tuple. Collect the statistics in an histogram and compute statistical estimators (e.g., the median). Two examples of the simulated PDT are shown in Sec. 3 of the main text (Fig. 3 and Fig. 4).

Appendix B. Application of the model to a satellite-based link

In this section we are going to apply the model described in the previous section to a satellite-based link, as described in Sec. 3 of the main text. We will discuss some details about the calculations involved and show an example of how to proceed with the integration of the expressions in Appendix A. In particular, we will focus on the first term of the quantity $\langle W_{1/2}^2 \rangle$ defined in equation Eq. (A.14), which only contains the second order correlation function $\Gamma_2(\boldsymbol{\rho}; L)$. The computations involving the integration of the fourth order correlation function $\Gamma_4(\boldsymbol{\rho}_1, \boldsymbol{\rho}_2; L)$ are much more cumbersome and will not be reported here.

Inserting Eq. (A.21) in the first term of Eq. (A.14) we obtain the following integration, where all the quantities are defined in the previous section Appendix A

$$\begin{aligned}\int_{\mathbb{R}^2} d^2\boldsymbol{\rho}\ x^2\ \Gamma_2(\boldsymbol{\rho}; L) = \frac{\Omega^2}{\pi^2 W_0^4} \int_{\mathbb{R}^4} d^2\boldsymbol{\rho}\ d^2\boldsymbol{\rho}'\ x^2\ \mathrm{e}^{-\frac{\alpha}{2W_0^2}|\boldsymbol{\rho}'|^2 - 2i\frac{\Omega}{W_0^2}\boldsymbol{\rho}\cdot\boldsymbol{\rho}'} \\ \exp\Big[-\frac{1}{2}\mathcal{D}_S^{\rm turb}(0, \boldsymbol{\rho}')\Big] \exp\Big[-\frac{1}{2}\mathcal{D}_S^{\rm scat}(0, \boldsymbol{\rho}')\Big]\ .\end{aligned} \tag{B.1}$$

We assume that the beam is focused ($F = L$) so that $\alpha = 1$. First of all we can compute the terms $\mathcal{D}_S^{\rm turb}(0, \boldsymbol{\rho}')$ and $\mathcal{D}_S^{\rm scat}(0, \boldsymbol{\rho}')$ defined in Eq. (A.19) and (A.20)

$$\mathcal{D}_S^{\rm turb}(0, \boldsymbol{\rho}') = 2.95\ k^2\ L \int_0^1 d\xi\ C_n^2(\xi)\ |\boldsymbol{\rho}'(1-\xi)|^{\frac{5}{3}} \tag{B.2}$$

$$\mathcal{D}_S^{\rm scat}(0, \boldsymbol{\rho}') = \frac{\pi}{8} L \int_0^1 d\xi\ n_0(\xi)\ |\boldsymbol{\rho}'(1-\xi)|^2\ . \tag{B.3}$$

In the rescaled longitudinal coordinate ξ, the conditions in Eq. (3) in the main text become

$$\begin{aligned} &\text{Down} - \text{links} && C_n^2(\xi) = C_n^2\ \Theta(\xi - (1 - h/L)) \\ & && n_0(\xi) = n_0\ \Theta(\xi - (1 - h/L)) \\ &\text{Up} - \text{links} && C_n^2(\xi) = C_n^2\ \Theta(h/L - \xi) \\ & && n_0(\xi) = n_0\ \Theta(h/L - \xi)\ . \end{aligned} \tag{B.4}$$

Inserting Eq. (B.4) (we consider down-link in this example) into Eq. (B.2) and (B.3) we can solve the integration and obtain

$$\begin{aligned} &\mathcal{D}_S^{\rm turb}(0, \boldsymbol{\rho}') = 2.95\ k^2\ L\ |\boldsymbol{\rho}'|^{\frac{5}{3}} C_n^2 \int_{1-h/L}^1 d\xi\ \ (1-\xi)^{\frac{5}{3}} \\ &= 2.4\ \sigma_R^2\ k^{5/6}\ L^{-5/6}\ |\boldsymbol{\rho}'|^{\frac{5}{3}} \Big[\frac{3}{8}\Big(\frac{h}{L}\Big)^{8/3}\Big] \end{aligned} \tag{B.5}$$

$$\begin{aligned} &\mathcal{D}_S^{\rm scat}(0, \boldsymbol{\rho}') = \frac{\pi}{8} L n_0 |\boldsymbol{\rho}'|^2 \int_{1-h/L}^1 d\xi\ \ |\boldsymbol{\rho}'(1-\xi)|^2 \\ &= \frac{\pi}{8} L n_0 |\boldsymbol{\rho}'|^2 \Big[\frac{1}{3}\Big(\frac{h}{L}\Big)^3\Big] \end{aligned} \tag{B.6}$$

where σ_R^2 has been defined in Sec. 3. From this passage we clearly see where the dependency on $\frac{h}{L}$ in Eq. (4) to Eq. (9) originates from. When we introduce Eq. (B.5) and Eq. (B.6) in Eq. (B.1), we recognize that it only contains Gaussian integrals of the form

$$\int_{-\infty}^{\infty} dx\ x^c\ \exp[a\ x^2 + i\ b\ x]\ , \tag{B.7}$$

with $c = \{0, 2\}$ and that can be readily solved. The only exception is the turbulence term, which contains $|\boldsymbol{\rho}'|^{\frac{5}{3}}$. We can simplify the computation introducing the approximation [22, 71] $|\boldsymbol{\rho}'/W_0|^{\frac{5}{3}} \simeq |\boldsymbol{\rho}'/W_0|^2$. Then, one just has to solve the multiple Gaussian integrals and insert it in Eq. (A.14) to obtain the value of $\langle W_{1/2}^2 \rangle$ for down-links, as in Eq. (8). Similar techniques can be used to compute all the other moments of the beam variables.

Eq. (4), (5), (7) and (8) have been computed specifically for the problem at hand, the non-uniform link described at the beginning of Sec. 3. Eq. (6) and (9), on the

other hand, have been deduced from the equivalent results obtained in [22] for a uniform link. We see that in Eq. (4), (5), (7) and (8) the corrections due to the non-uniformity of the link (of the form $A(h/L)^{\beta}$, where A is a constant and $\beta = \{1, 8/3, 3\}$) act like multiplicative factors on the parameters σ_R^2 and n_0. So, we started from the calculation of the quantity $\langle \Delta W_i^2 \Delta W_j^2 \rangle$ in [22] and attached the multiplicative corrections found above, in order to obtain Eq. (6) and (9). This inconsistency should not be considered too detrimental regarding the reliability of the model. We checked through the simulation that the mean value and the shape of the PDT are not very sensitive to variations of the value of the quantities in Eq. (6) and (9), as the interplay between beam wandering (Eq. (4) and (7)) and beam spreading (Eq. (5) and (8)) is much more significant in this context. Finally, we point out that the computation of the quantities in Eq. (4), (5), (7) and (8) have been carried out without the introduction of the weak turbulence approximation used in [21, 22]. For Eq. (6) and (9), instead, we used the results obtained in [22] in the weak turbulence regime, which we verified to be still valid in the case of satellite-based links.

Appendix C. Error model and environmental photons

In a free-space link, environmental photons are usually the most important source of noise. In this section we summarize the analysis of [11, 23] regarding the amount of environmental photons that hit the detector for down-links and up-links, that we use to calculate the Quantum Bit Error Rate (QBER). We suppose that an accurate time synchronization had been operated between sender and receiver, in order to tag the photons and perform a time filtering on the incoming signal. On top of that, wavelength filtering is applied to further reduce the amount of detected noisy photons.

For up-links, we only consider the case of night-time operation. If the ground station site has a low level of light pollution, the biggest fraction of environmental photons comes from the Sunlight reflected first by the Moon and then by the Earth [11]

$$N_{\text{night}}^{\text{up}} = A_E A_M R_M^2 a^2 \frac{\Omega_{\text{fov}}}{d_{EM}^2} B_f \ \Delta t \ H_{\text{sun}} \ . \tag{C.1}$$

Here A_M and R_M are the albedo and the radius of the Moon, while A_E is the albedo of the Earth and d_{EM} is the Earth-Moon distance. H_{sun} is the solar spectral irradiance in photons $\text{s}^{-1}\text{nm}^{-1}\text{m}^{-2}$ at the wavelength of interest. Ω_{fov} and a are angular field of view and radius of the receiving telescope. B_f is the width of the spectral filtering and Δt is the detection time-window. We assumed Lambertian diffusion on the Moon and the Earth.

For down-links, the evaluation of the background photons is strongly site-dependent. The power received by the telescope can be expressed as follows [23]

$$P_b = H_b \Omega_{\text{fov}} \pi a^2 B_f \ . \tag{C.2}$$

The parameter H_b is the total brightness of the sky background and it depends on the hour of the day and the weather conditions. From Eq. (C.2) we derive the number of

photons per time window

$$N^{\rm down} = \frac{H_b}{h\nu}\Omega_{\rm fov}\pi a^2 B_f\ \Delta t\ , \tag{C.3}$$

where h is the Planck constant and ν is the frequency of the background photons (after filtering). Typical values of the brightness of the sky are $H_b = 10^{-3}\ W\ {\rm m}^{-2}$ sr μm during a full-Moon night and $H_b = 1\ W\ {\rm m}^{-2}$ sr μm for a clear sky in day-time. This analysis assumes that neither the Moon during the night nor the Sun during the day are included in the field of view of the collecting aperture.

The Quantum bit error rate is computed assuming the noisy photons to be completely unpolarized

$$QBER = Q_0 + \frac{1}{2}\frac{N_{\rm noise}}{N_{\rm noise}+N_{\rm sig}}\ . \tag{C.4}$$

Here Q_0 corresponds to the error rate associated with depolarization in the encoding degree of freedom or imperfection of the preparation or detection stage leading to incorrect state discrimination. We chose a conservative value of $Q_0 = 2\%$. $N_{\rm noise}$ and $N_{\rm sig}$ are, respectively, the number of photons per time window associated to noise and signal. As expected, the number of collected environmental photons are proportional to the area of the receiving aperture, but so is the intensity of the signal. To reduce the noise and at the same time raise the signal to noise ratio, we can act on $\Omega_{\rm fov}$, B_f and Δt. Reducing the field of view involves a better pointing and tracking system, while a very good time synchronization allows the use of short time windows.

Appendix D. Rates for BB-84 with single photons and Weak Coherent Pulses

We report here the expression of the secret key rates we used in the performance study of section 4. The set-up is the usual one for QKD: two parties, A and B, are connected through a completely insecure quantum channel and an authenticated classical channel. After many uses of the links, their goal is to share an identical key, which is secret regardless of the attack strategy that an hypothetical eavesdropper could implement. For the single-photon implementation of the BB-84 protocol (using, e.g., polarization encoding), party A sends qubits in the basis $X = \{|0\rangle, |1\rangle\}$ or $Z = \{|+\rangle, |-\rangle\}$ at random, with $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. B measures the received qubits in the bases X or Z, at random. The results of [53] state that a secret key of length l can be shared, if

$$\begin{aligned} &l \leq n(q - h_2(Q_{\rm tol}+\mu)) - {\rm leak}_{EC} - \alpha(\varepsilon_{\rm sec},\varepsilon_{\rm cor}) \\ &\alpha(\varepsilon_{\rm sec},\varepsilon_{\rm cor}) = \log_2\frac{2}{\varepsilon_{\rm sec}^2\varepsilon_{\rm cor}}\quad \mu = \sqrt{\frac{n+k}{nk}\frac{k+1}{k}\ln\frac{2}{\varepsilon_{\rm sec}}}\ , \end{aligned} \tag{D.1}$$

out of n successfully exchanged single photon signals, where the function h_2 denotes the binary entropy. Here q is a parameter describing the preparation quality of the initial states of the signal sent by A. In the qubit case it is connected to the maximum fidelity

allowed between states prepared in the X and Z bases. In a perfect implementation of the BB-84 protocol, like the one considered here, the two bases are mutually unbiased, for which the maximum $q = 1$ is achieved. $Q_{\rm tol}$ is the channel error tolerance and k is the number of bits of the raw key used for parameter estimation. The achievable key rate is obtained by maximizing over these two parameters. The term leak_{EC} gives the amount of information in bits that the parties had to exchange during the error correction phase. The desired security and correctness thresholds are specified by the parameters $\varepsilon_{\rm sec}$ and $\varepsilon_{\rm cor}$.

An alternative protocol based on decoy states [54, 56] is used when the source emits Weak Coherent Pulses instead of real single photons. We follow the analysis of [55, 57], where two decoy states are used. The bases used for the encoding are X and Z as in the single photon implementation. A secret key of length l can be extracted, with

$$l \leq s_{X,0} + s_{X,1}(1 - h_2(\phi_X)) - \text{leak}_{EC} - 6\ \log_2 \frac{21}{\varepsilon_{\rm sec}} - \log_2 \frac{2}{\varepsilon_{\rm cor}}\ . \qquad \text{(D.2)}$$

$s_{X,0}$ and $s_{X,1}$ represent the number of bits in the raw key generated by vacuum events and single photon events, respectively. ϕ_X instead is the phase error rate measured in the channel during parameter estimation. The subscript X means that these estimations are valid for the events in which both A and B chose the basis X and they include the corrections due to finite key effects (for the actual expressions we refer to [57]). In this case the maximization is over the portion of signals used for parameter estimation, the intensity of the signal and decoy states and the probability of sending different intensities.

In both cases, the key rates are obtained taking the ratio between the length in bit of the final secret key l and total number of signals sent n.

Appendix E. Choice of parameters for the satellite-based link

In this section we show the values oft the parameters utilized throughout the paper and we discuss about their pertinence. They are reported in Tab. E1, Tab. E2 and Tab. E3, together with a brief explanatory description, where necessary. More detailed explanations about particular parameters are in the remainder of this section.

The parameters C_n^2, n_0 and h should in general be fixed by fitting the experimental data. However, in order to have a predictive model, we want to estimate these parameters in a reasonable way. First of all, in order to estimate the effective thickness of the atmosphere, we start from the variation of density of the air as a function of the altitude. We chose $h = 20$ km, as a layer around the Earth with this thickness contains on average 95% of the total mass of the atmosphere. As already stated in the main text, some models for the altitude dependence of the refractive index structure constant C_n^2 are available in the literature [34, 35, 36, 37]. The widely used parametric fit due to Hufnagel and Valley [34, 35] reliably replicates the behaviour of C_n^2 in mid-latitude climate

Parameter	Value	Brief description
W_0	15 cm, 50 cm	down-links, up-links
W_0	5 cm, 50 cm	CubeSat down-links, up-links
a	50 cm, 15 cm	down-links, up-links
a	50 cm, 5 cm	CubeSat down-links, up-links
λ	785 nm	Wavelength of the signal light
β	0.7	Parameter in $\chi_{\rm ext}(\theta)$
α	1.2 10^{-6} rad	Pointing error
$\eta_{\rm det}$	0.5	Detector efficiency
$T_{\rm opt}$	0.8	Transmittance of the optical system

Table E1. Parameters related to the optical and technical properties of the link.

Parameter	Value	Brief description
h	20 km	Atmosphere thickness
L	500 km	Minimum altitude (zenith)
C_n^2	1.12 10^{-16} m$^{-2/3}$	Night-time, condition 1
C_n^2	1.64 10^{-16} m$^{-2/3}$	Day-time, condition 1
C_n^2	5.50 10^{-16} m$^{-2/3}$	Night-time, condition 2
C_n^2	8.00 10^{-16} m$^{-2/3}$	Day-time, condition 2
C_n^2	1.10 10^{-15} m$^{-2/3}$	Night-time, condition 3
C_n^2	1.60 10^{-15} m$^{-2/3}$	Day-time, condition 3
n_0	0.61 m^{-3}	Night-time, condition 1
n_0	0.01 m^{-3}	Day-time, condition 1
n_0	3.00 m^{-3}	Night-time, condition 2
n_0	0.05 m^{-3}	Day-time, condition 2
n_0	6.10 m^{-3}	Night-time, condition 3
n_0	0.10 m^{-3}	Day-time, condition 3

Table E2. Parameters related to the atmospheric weather conditions.

$$C_n^2(z) = 5.94\ 10^{-53}\Big(\frac{v}{27}\Big)^2 z^{10}\ \exp[-z/1000] + \\ + 2.7\ 10^{-16}\ \exp[z/1500] + A\ \exp[z/100]\ . \tag{E.1}$$

Here z is the altitude coordinate, v is a parameter related to high-altitude wind speed and A describes the relative strength of the turbulence near the ground level. Typical values are $A = 1.7\ 10^{-14}$ m$^{-2/3}$ and $v = 21$ m/s, although $v = 57$m/s is sometimes used for stronger wind conditions. The value of C_n^2 inside the atmosphere in our model is estimated by the integral average of this function in $[0, \infty]$, rescaled by the fixed thickness h

$$C_n^2 = \frac{1}{h}\int_0^\infty C_n^2(z)\ dz\ . \tag{E.2}$$

Parameter	Value	Brief description
Sky brightness H_b	1.5 10^{-6} W m^{-2} sr^{-1}nm^{-1}	Night, clear sky, full Moon [23]
Sky brightness H_b	1.5 10^{-3} W m^{-2} sr^{-1}nm^{-1}	Day, clear sky [23]
Field of view $\Omega_{\rm fov}$	$(100\ 10^{-6})^2$ sr	Night-time down-link
Field of view $\Omega_{\rm fov}$	$(10\ 10^{-6})^2$ sr	Day-time down-link
Field of view $\Omega_{\rm fov}$	$(30\ 10^{-6})^2$ sr	Night-time up-link
Time-window Δt	1 ns	Night- and day-time
Spectral filter width B_f	1 nm	Night-time down-link
Spectral filter width B_f	0.2 nm	Day-time down-link
Spectral filter width B_f	1 nm	Night-time up-link
$H_{\rm sun}$	4.610 10^{18} phot s^{-1}nm^{-1}m^{-2}	Solar spectral irradiance
A_e	0.300	Earth's albedo
A_m	0.136	Moon's albedo
R_M	1.737 10^6 m	Moon's radius
d_{EM}	3.600 10^8 m	Earth-Moon distance

Table E3. Parameters related to stray photons and environmental light.

The parameter v is kept fixed to the recommended value of 21 m/s. A is chosen to match the values of $C_n^2(0)$ measured in [22], $A_n = 1.10\ 10^{-14}$ m$^{-2/3}$ at night and $A_d = 2.75\ 10^{-14}$ m$^{-2/3}$ during the day. Through Eq. (E.1), the first corresponds to $C_n^2 = 1.12\ 10^{-16}$ m$^{-2/3}$ and the latter to $C_n^2 = 1.64\ 10^{-16}$ m$^{-2/3}$.

The scattering particles described by the density n_0 mainly consist of water droplets, so, in order to estimate the value of n_0, we start from the profile of the water vapour content in the atmosphere. The absolute humidity vertical profile $\tau(z)$ in the range $[0, 10\ \text{km}]$ can be written as a double exponential [72, 73]

$$\begin{aligned} \tau(z) &= \tau(0)\ \exp[-z/H_1] && \text{for } 0 \le z \le 5\ \text{km} \\ &= \tau(H_1)\ \exp[-(z-5\ \text{km})/H_2] && \text{for } 5\ \text{km} \le z \le 10\ \text{km} \end{aligned} \tag{E.3}$$

with the two scale heights H_1 and H_2. The contribution of the region with $z > 10$ km is rather low and we neglect it here. The parameters H_1 and H_1 can on average vary in the range $[1.53, 2.8]$ and $[1.19, 1.82]$, respectively, depending on the geographical position and the season. We choose in the following the values stated in the U. S. Standard Atmosphere (1962) [74], $H_1 = 2.243$ and $H_2 = 1.414$. We obtain a rescaling factor ω in the same way as we did in the previous case

$$\omega = \frac{1}{h\ \tau(0)} \int_0^{10\ \text{km}} \tau(z)\ dz\ . \tag{E.4}$$

Then, the value of the parameter n_0^* in our case is obtained multiplying by the factor ω the value found in [22] for night- and day-time, $n_0^* = \omega\ n_0$. For the given values of the scale heights $\omega \simeq 0.107$.

The extinction factor $\chi_{\rm ext}(\theta)$ varies as a function of the elevation angle in the following way

$$\chi_{\rm ext}(\theta) = \exp[-\beta \sec(\theta)] \tag{E.5}$$

The value of the parameter β reported in Tab. E1 has been chosen to match the amount of extinction used in [10], based on the MODTRAN5 software [38].

[1] M. Minder et al. Experimental quantum key distribution beyond the repeaterless secret key capacity. *Nature Photonics*, 13(5):334–338, 2019.

[2] A. Boaron et al. Secure quantum key distribution over 421 km of optical fiber. *Phys. Rev. Lett.*, 121:190502, Nov 2018.

[3] W. J. Munro, K. Azuma, K. Tamaki, and K. Nemoto. Inside quantum repeaters. *IEEE Journal of Selected Topics in Quantum Electronics*, 21(3):78–90, May 2015.

[4] K. Azuma, K. Tamaki, and H.-K. Lo. All-photonic quantum repeaters. *Nature Communications*, 6:6787 EP –, Apr 2015. Article.

[5] M. Zwerger, A. Pirker, V. Dunjko, H. J. Briegel, and W. Dür. Long-range big quantum-data transmission. *Phys. Rev. Lett.*, 120:030503, Jan 2018.

[6] Z. Su, J. Guan, and L. Li. Efficient quantum repeater with respect to both entanglement-concentration rate and complexity of local operations and classical communication. *Phys. Rev. A*, 97:012325, Jan 2018.

[7] N. Sangouard, C. Simon, H. de Riedmatten, and N. Gisin. Quantum repeaters based on atomic ensembles and linear optics. *Rev. Mod. Phys.*, 83:33–80, Mar 2011.

[8] K. Boone, J.-P. Bourgoin, E. Meyer-Scott, K. Heshami, T. Jennewein, and C. Simon. Entanglement over global distances via quantum repeaters with satellite links. *Phys. Rev. A*, 91:052325, May 2015.

[9] R. Bedington, J. M. Arrazola, and A. Ling. Progress in satellite quantum key distribution. *npj Quantum Information*, 3(1):30, 2017.

[10] J.-P. Bourgoin et al. A comprehensive design and performance analysis of low earth orbit satellite quantum communication. *New Journal of Physics*, 15(2):023006, 2013.

[11] C. Bonato, A. Tomaello, V. Da Deppo, G. Naletto, and P. Villoresi. Feasibility of satellite quantum key distribution. *New Journal of Physics*, 11(4):045017, 2009.

[12] S.-K. Liao et al. Satellite-to-ground quantum key distribution. *Nature*, 549:43 EP –, Aug 2017. Article.

[13] J. Yin et al. Satellite-to-ground entanglement-based quantum key distribution. *Phys. Rev. Lett.*, 119:200501, Nov 2017.

[14] J.-G. Ren et al. Ground-to-satellite quantum teleportation. *Nature*, 549:70 EP –, Aug 2017.

[15] J. Yin et al. Satellite-based entanglement distribution over 1200 kilometers. *Science*, 356(6343):1140–1144, 2017.

[16] H. Takenaka, A. Carrasco-Casado, M. Fujiwara, M. Kitamura, M. Sasaki, and M. Toyoshima. Satellite-to-ground quantum-limited communication using a 50-kg-class microsatellite. *Nature Photonics*, 11:502 EP, Jul 2017. Article.

[17] S. Slobin S. Piazzolla. Statistics of link blockage due to cloud cover for free-space optical communications using ncdc surface weather observation data, 2002.

[18] A. Viswanath, V. K. Jain, and S. Kar. Analysis of earth-to-satellite free-space optical link performance in the presence of turbulence, beam-wander induced pointing error and weather conditions for different intensity modulation schemes. *IET Communications*, 9(18):2253–2258, 2015.

[19] H. Li, Y. Huang, Q. Wang, D. He, Z. Peng, and Q. Li. Performance analysis of satellite-to-ground coherent optical communication system with aperture averaging. *Applied Sciences*, 8(12), 2018.

[20] H. Kaushal and G. Kaddoum. Optical communication in space: Challenges and mitigation techniques. *IEEE Communications Surveys Tutorials*, 19(1):57–96, Firstquarter 2017.

[21] D. Vasylyev, A. A. Semenov, and W. Vogel. Atmospheric quantum channels with weak and strong turbulence. *Phys. Rev. Lett.*, 117:090501, Aug 2016.

[22] D. Vasylyev et al. Free-space quantum links under diverse weather conditions. *Phys. Rev. A*, 96:043856, Oct 2017.

[23] E.-L. Miao, Z.-F. Han, S.-S. Gong, T. Zhang, D.-S. Diao, and G.-C. Guo. Background noise of satellite-to-ground quantum key distribution. *New Journal of Physics*, 7(1):215, 2005.

[24] A. N. Kolmogorov. Local structure of turbulence in an incompressible viscous fluid at very high

reynolds numbers. *Soviet Physics Uspekhi*, 10(6):734, 1968.

[25] R. L. Fante. Electromagnetic beam propagation in turbulent media: An update. *Proceedings of the IEEE*, 68(11):1424–1443, Nov 1980.

[26] V. A. Banakh and V. L. Mironov. Phase approximation of the huygens–kirchhoff method in problems of laser-beam propagation in the turbulent atmosphere. *Opt. Lett.*, 1(5):172–174, Nov 1977.

[27] V. I. Tatarskii. *The effects of the turbulent atmosphere on wave propagation*. Jerusalem: Israel Program for Scientific Translations. 1971.

[28] A. Deepak, U. O. Farrukh, and A. Zardecki. Significance of higher-order multiple scattering for laser beam propagation through hazes, fogs, and clouds. *Appl. Opt.*, 21(3):439–447, Feb 1982.

[29] M. Grabner and V. Kvicera. Multiple scattering in rain and fog on free-space optical links. *Journal of Lightwave Technology*, 32(3):513–520, Feb 2014.

[30] I. P. Lukin. Random displacements of optical beams in an aerosol atmosphere. *Radiophys. Quantum Electron.*, 24(95), 1981.

[31] H. T. Yura, K. G. Barthel, and W. Büchtemann. Rainfall-induced optical phase fluctuations in the atmosphere. *J. Opt. Soc. Am.*, 73(11):1574–1580, Nov 1983.

[32] I. P. Lukin, D. S. Rychkov, A. V. Falits, K. S. Lai, and M. R. Liu. A phase screen model for simulating numerically the propagation of a laser beam in rain. *Quantum Electronics*, 39(9):863, 2009.

[33] H. Hemmati. *Near-Earth Laser Communications*. Optical Science and Engineering. CRC Press, 2009.

[34] R. E. Hufnagel and N. R. Stanley. Modulation transfer function associated with image transmission through turbulent media. *J. Opt. Soc. Am.*, 54(1):52–61, Jan 1964.

[35] G. C. Valley. Isoplanatic degradation of tilt correction and short-term imaging systems. *Appl. Opt.*, 19(4):574–577, Feb 1980.

[36] J. K. Lawson and C. J. Carrano. Using historic models of C_n^2 to predict r_0 and regimes affected by atmospheric turbulence for horizontal, slant, and topological paths. *Proc.SPIE*, 6303:6303 – 6303 – 12, 2006.

[37] R. Frehlich et al. Estimates of cn2 from numerical weather prediction model output and comparison with thermosonde data. *Journal of Applied Meteorology and Climatology*, 49(8):1742–1755, 2010.

[38] Ontar corporation. https://ontar.com.

[39] D. Vasylyev, W. Vogel, and F. Moll. Satellite-mediated quantum atmospheric links. *Phys. Rev. A*, 99:053830, May 2019.

[40] M. Aspelmeyer, T. Jennewein, M. Pfennigbauer, W. R. Leeb, and A. Zeilinger. Long-distance quantum communication with entangled photons using satellites. *IEEE Journal of Selected Topics in Quantum Electronics*, 9(6):1541–1551, Nov 2003.

[41] F. Dios, J. Recolons, A. Rodríguez, and O. Batet. Temporal analysis of laser beam propagation in the atmosphere using computer-generated long phase screens. *Opt. Express*, 16(3):2206–2220, Feb 2008.

[42] F. Dios J. Recolons. Accurate calculation of phase screens for the modelling of laser beam propagation through atmospheric turbulence, 2005.

[43] Y. Cao, S. L. Dvorak, X. Ye, and B. Herman. A new cylindrical phase screen method for modeling electromagnetic wave propagation through an inhomogeneous 2-d atmosphere. *Radio Science*, 42(4).

[44] E. Limpert, M. Abbt, and W. A. Stahel. Log-normal Distributions across the Sciences: Keys and Clues. *BioScience*, 51(5):341–352, 05 2001.

[45] A.N. Stassinakis, H.E. Nistazakis, K.P. Peppas, and G.S. Tombras. Improving the availability of terrestrial fso links over log normal atmospheric turbulence channels using dispersive chirped gaussian pulses. *Optics & Laser Technology*, 54:329 – 334, 2013.

[46] R. L. Phillips A. Al-Habash, L. C. Andrews. Mathematical model for the irradiance probability density function of a laser beam propagating through turbulent media. *Optical Engineering*,

40:40 – 40 – 9, 2001.

[47] N. D. Chatzidiamantis, H. G. Sandalidis, G. K. Karagiannidis, S. A. Kotsopoulos, and M. Matthaiou. New results on turbulence modeling for free-space optical systems. In *2010 17th International Conference on Telecommunications*, pages 487–492, April 2010.

[48] G. Vallone et al. Adaptive real time selection for quantum key distribution in lossy and turbulent free-space channels. *Phys. Rev. A*, 91:042320, Apr 2015.

[49] W. Wang, F. Xu, and H.-K. Lo. Prefixed-threshold real-time selection method in free-space quantum key distribution. *Phys. Rev. A*, 97:032337, Mar 2018.

[50] C. Erven et al. Studying free-space transmission statistics and improving free-space quantum key distribution in the turbulent atmosphere. *New Journal of Physics*, 14(12):123018, 2012.

[51] X.-L. Hu, Y. Cao, Z.-W. Yu, and X.-B. Wang. Measurement-device-independent quantum key distribution over asymmetric channel and unstable channel. *Scientific Reports*, 8(1):17634, 2018.

[52] C.H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore*, pages 175–179, 1984.

[53] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner. Tight finite-key analysis for quantum cryptography. *Nat Commun*, 3:634, Jan 2012.

[54] X.-B. Wang. Beating the photon-number-splitting attack in practical quantum cryptography. *Phys. Rev. Lett.*, 94:230503, Jun 2005.

[55] H.-K. Lo, X. Ma, and K. Chen. Decoy state quantum key distribution. *Phys. Rev. Lett.*, 94:230504, Jun 2005.

[56] X.-B. Wang, T. Hiroshima, A. Tomita, and M. Hayashi. Quantum information with gaussian states. *Physics Reports*, 448(1):1 – 111, 2007.

[57] C. C. W. Lim, M. Curty, N. Walenta, F. Xu, and H. Zbinden. Concise security bounds for practical decoy-state quantum key distribution. *Phys. Rev. A*, 89:022307, Feb 2014.

[58] E. L. Shkolnik. On the verge of an astronomy cubesat revolution. *Nature Astronomy*, 2(5):374–378, 2018.

[59] A. Poghosyan and A. Golkar. Cubesat evolution: Analyzing cubesat capabilities for conducting science missions. *Progress in Aerospace Sciences*, 88:59 – 83, 2017.

[60] W. A. Shiroma et al. CubeSats: A bright future for nanosatellites. *Central European Journal of Engineering*, 1:9–15, March 2011.

[61] D. K. L. Oi et al. Cubesat quantum communications mission. *EPJ Quantum Technology*, 4(1):6, Apr 2017.

[62] J. A. Grieve, R. Bedington, Z. Tang, R. C.M.R.B. Chandrasekara, and A. Ling. Spooqysats: Cubesats to demonstrate quantum key distribution technologies. *Acta Astronautica*, 151:103 – 106, 2018.

[63] E. Kerstel et al. Nanobob: a cubesat mission concept for quantum communication experiments in an uplink configuration. *EPJ Quantum Technology*, 5(1):6, Jun 2018.

[64] S. P. Neumann et al. Q3sat: quantum communications uplink to a 3u cubesat-feasibility & design. *EPJ Quantum Technology*, 5(1):4, Apr 2018.

[65] S. Wengerowsky, S. K. Joshi, F. Steinlechner, H. Hübel, and R. Ursin. An entanglement-based wavelength-multiplexed quantum communication network. *Nature*, 564(7735):225–228, 2018.

[66] S. Wehner, D. Elkouss, and R. Hanson. Quantum internet: A vision for the road ahead. *Science*, 362(6412), 2018.

[67] A. Dahlberg, M. Skrzypczyk, T. Coopmans, L. Wubben, F. Rozpedek, M. Pompili, A. Stolk, P. Pawełczak, R. Knegjens, J. de Oliveira Filho, R. Hanson, and S. Wehner. A Link Layer Protocol for Quantum Networks. *arXiv e-prints*, page arXiv:1903.09778, Mar 2019.

[68] T. Vergoossen, S. Loarte, R. Bedington, H. Kuiper, and A. Ling. Satellite constellations for trusted node QKD networks. *arXiv e-prints*, page arXiv:1903.07845, Mar 2019.

[69] K. Boone, J.-P. Bourgoin, E. Meyer-Scott, K. Heshami, T. Jennewein, and C. Simon. Entanglement over global distances via quantum repeaters with satellite links. *Phys. Rev. A*,

91:052325, May 2015.

[70] V. A. Banakh and V. L. Mironov. Phase approximation of the huygens–kirchhoff method in problems of laser-beam propagation in the turbulent atmosphere. *Opt. Lett.*, 1(5):172–174, Nov 1977.

[71] L. C. Andrews and R. L. Phillips. *Laser Beam Propagation through Random Media, Second Edition*. SPIE Press, 2005.

[72] C. Tomasi and T. Paccagnella. Vertical distribution features of atmospheric water vapour in the Po valley area. *Pure and Applied Geophysics*, 127(1):93–115, Mar 1988.

[73] C. Tomasi. Vertical distribution features of atmospheric water vapor in the mediterranean, red sea, and indian ocean. *Journal of Geophysical Research: Atmospheres*, 89(D2):2563–2566.

[74] N. Sissenwine, M. Dubin, and H. Wexler. The u.s. standard atmosphere, 1962. *Journal of Geophysical Research (1896-1977)*, 67(9):3627–3630, 1962.

Paper 2

The material in this chapter has been reproduced from the following preprint [20]:

Carlo Liorni, Hermann Kampermann and Dagmar Bruß, *Quantum repeaters in space*, arXiv:2005.10146, 2020

Quantum repeaters in space

Carlo Liorni[1*], Hermann Kampermann[1], Dagmar Bruß[1]

[1]Heinrich-Heine-Universität, Institut für Theoretische Physik III, Universitätsstr. 1, 40225, Düsseldorf, Germany. Correspondence and requests for materials should be addressed to C.L. (email: liorni@uni-duesseldorf.de)

Abstract

Long-distance entanglement is a very precious resource, but its distribution is very difficult due to the exponential losses of light in optical fibres. A possible solution consists in the use of quantum repeaters, based on entanglement swapping or quantum error correction. Alternatively, satellite-based free-space optical links can be exploited, achieving better loss-distance scaling. We propose to combine these two ingredients, quantum repeaters and satellite-based links, into a scheme that allows to achieve entanglement distribution over global distances with a small number of intermediate untrusted nodes. The entanglement sources, placed on satellites, send quantum states encoded in photons towards orbiting quantum repeater stations, where entanglement swapping is performed. The performance of this repeater chain is assessed in terms of the secret key rate achievable by the BB-84 cryptographic protocol. We perform a comparison with other repeater chain architectures and show that our scheme, even though more technically demanding, is superior in many situations of interest. Finally, we analyse strengths and weaknesses of the proposed scheme and discuss exemplary orbital configurations. The integration of satellite-based links with ground repeater networks can be envisaged to represent the backbone of the future Quantum Internet.

Keywords: Satellite links, Quantum repeaters, Quantum networks, Quantum Key Distribution, Quantum Internet

Entanglement distribution between very distant parties allows several interesting quantum-enabled protocols to be performed, in the fields of quantum communication [1, 2], metrology [3, 4, 5] and distributed computation [6, 7]. However, achieving this task over global distances (thousands of km) is very daunting. The standard carrier of quantum information is light, sent through optical fibres. The exponential losses experienced during the propagation limit the achievable distances to $\sim$ 200 km in practice. The concept of a Quantum Repeater (QR) [8, 9, 10, 11, 12, 13] has been introduced to counter this problem. Such a device allows, using Quantum Memories (QMs) [14] and protocols based on Entanglement Swapping (ES) or quantum error correction [15], to connect several elementary links and enlarge the achievable distance.

An alternative solution is represented by satellite-relayed free-space channels. Satellite-to-ground optical links for quantum communication have already been proven to be feasible with current technology [16, 17, 18, 19] and have been the object of a plethora of theoretical studies [20, 21, 22, 23, 24, 25, 26, 27]. They allow, in the double down-link configuration, to share entanglement between two ground stations, at distances that far exceed what can be achieved with direct fibre transmission. Low Earth Orbit (LEO, altitude $\lesssim$ 2000 km) satellites are preferred, because of the lower cost and the shorter distance between the satellite and the ground stations, which reduces the overall loss in the channel. However, the maximum distance between the ground stations is limited to $\{1500-2000\}$ km, due to the additional losses encountered at low elevation angles. This aspect makes intercontinental quantum communication not feasible with such a scheme.

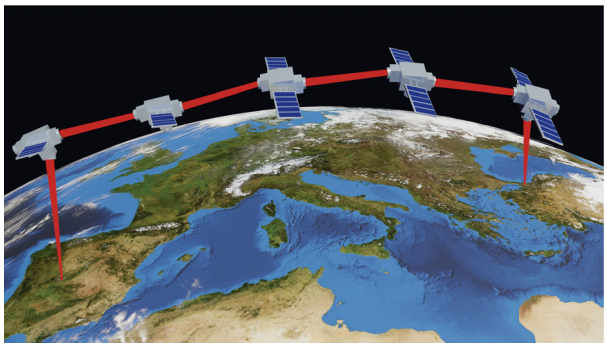

Figure 1: Pictorial representation of the scheme proposed in this paper for long-distance entanglement distribution, based on orbiting quantum repeater stations.

Through quantum repeaters, few of these satellite links can be chained together to reach global distances. In this work we propose and study the scheme pictured in Fig. 1, in which entanglement sources and quantum repeaters are placed on board of satellites, orbiting around the Earth in the *string of pearls* configuration. This allows to connect two users on the ground via free-space optical links outside the atmosphere, achieving far superior distance-to-loss ratio with respect to the standard fibre-based implementation. In this way, a small number of intermediate nodes is enough to achieve entanglement distribution over global distances at a reasonable rate.

We focus in the following on a specific application of entanglement distribution, namely Quantum Key Distribution (QKD). The secret key rate turns out to be a good measure of the effectiveness of the quantum repeater link [28]. We compare the performance of the newly-proposed scheme with two other quantum repeater configurations based on entanglement swapping. The nomenclature used in the remainder of the paper is the following, also schematically represented in Fig. 2: scheme OO (Orbiting sources Orbiting repeaters) is our proposal, scheme GG (Ground sources Ground repeaters) is the fibre-based one and scheme OG (Orbiting sources Ground repeaters) is the solution proposed in [22] (and expanded in [26]), where the quantum repeater stations are on the ground. We show that the configuration proposed and analysed here might represent a useful building block for the future global quantum network, once the additional technical requirements are met. A full satellite constellation study will be necessary, however, in order to fully grasp the potential of this scheme for real-life applications.

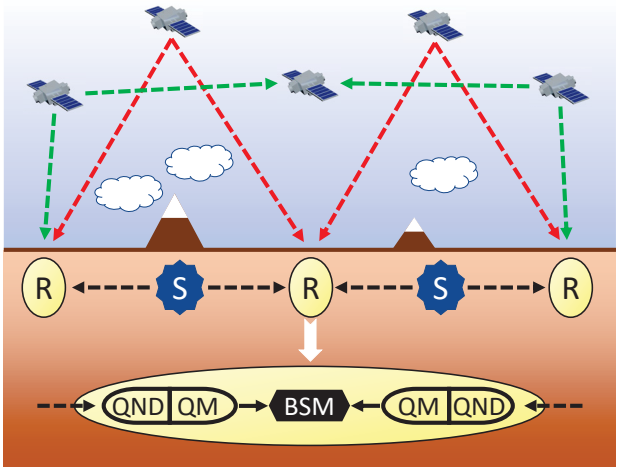

Figure 2: Schematic comparison between the satellite-based scheme OO (green arrows), the standard fibre-based implementation (GG, in black) and the scheme studied in [22] (OG, in red). Here S represent entanglement sources and R quantum repeater stations. The incoming photons are heralded by Quantum Non-Demolition meaurement devices (QND) and the quantum information is loaded into Quantum Memories (QM). Finally, the quantum states are read and a Bell State Measurement (BSM) is performed, as part of the entanglement swapping protocol.

In Sec. 1.1 we quantitatively estimate the performance of the different schemes in terms of achievable secret key rate and compare them. Afterwards, in Sec. 1.2, we discuss pros and cons of the proposed

satellite-based scheme and then analyse exemplary orbital configurations in Sec. 1.3. The results are briefly summarized and discussed in the conclusion, Sec. 2. Additional details on the simulations can be found in Sec. 3, regarding the error model and the contribution of environmental photons, the analysis of the orbits, the estimation of the satellite link transmittance and the values of the parameters used.

1 Results

1.1 Secret key rate and comparison

The quantum repeater architecture is designed as follows [29]. The total link of length L between the two communicating parties A and B is divided into 2^n elementary links of length $l_0 = L/2^n$. Quantum repeaters are placed at the connections between adjacent elementary links, while entanglement sources are in their central points (Fig. 2). The latter produce bipartite entangled states (in the following we will consider qubit pairs), encoded in some degree of freedom of a pair of photons, that are then injected in the adjacent elementary links. The quantum repeaters consist of 3 main devices. First of all Quantum Non-Demolition (QND) measurement devices herald the arrival of a photon from the elementary link. The quantum state encoded in the heralded photons is then loaded and stored in quantum memories. When both memories are full, a joint Bell State Measurement (BSM) is performed and the result broadcast. This entanglement swapping procedure allows to connect two adjacent entangled pairs and, repeated in a recursive and hierarchical way, to gradually extend the entanglement (see [28] for details). In consecutive *nesting levels*, the distance between the subsystems composing the entangled pairs will be doubled, with n the maximal nesting level. After n successful steps the entanglement is shared between the end points of the chain, the parties A and B.

In the case of scheme OO, the elementary links consist of double inter-satellite links and hybrid inter-satellite/down-link at the end points. In scheme GG, instead, they consist of optical fibres, whose transmittance $\eta_f(l) = 10^{-\alpha l/10}$ decreases exponentially with the length l, where the attenuation parameter is $\alpha = 0.17$ dB/km at 1550nm. Scheme OG on the other hand comprises double down-links from the satellites towards two adjacent receiving stations on the ground (as in Fig. 2). We discuss the losses introduced by such satellite links in Sec. 3.2. After an entangled pair is successfully shared between the parties A and B, it can be used for any quantum information protocol, in particular QKD. In this cryptographic primitive the two parties are connected by an insecure quantum link, the repeater chain, and by an authenticated classical channel. An eavesdropper can tamper on the classical channel and freely interact with the states sent over the quantum channel. The parties have to devise a protocol that either creates a private key or aborts. A generic protocol usually comprises the exchange of quantum states with successive measurements in random bases, base sifting, parameter estimation, error correction and privacy amplification. In the following we apply the well known asymmetric BB84 protocol (see [30] for the first proposal, [31] for the efficient asymmetric version and [32] for the entanglement-based scheme, also referred to as BBM92). In this protocol the quantum states are measured in the bases defined by the eigenstates of the X and Z Pauli operators on qubits. For the security analysis [28] we assume that the whole quantum repeater chain is untrusted, so, not only the quantum channels, but also the sources on the satellites and the repeater stations can be in the eavesdropper's hands. Our analysis of the repeater chain is not linked to any specific implementation regarding the encoding of the quantum information in the single photons. The choice of the encoding also depends on the chosen quantum memory architecture and material. For the satellite-based schemes polarization encoding is feasible [16, 17, 18, 19] and promising, so we base the error model on this assumption. Furthermore, we fix the wavelength of the photons to $\lambda = 580$nm, as discussed in Appendix Sec. 3.2. The secret key rate depends on both the repeater rate and the quality of the final shared entangled state. It is estimated in the limit of an infinitely long key, based on the considerations in [28], by:

$$R_{QKD}^{BB84} = R_{\text{rep}}\ P_{\text{click}}\ R_{\text{sift}}\ r_{\infty}^{BB84}\ . \tag{1}$$

In the expression above, R_{rep} represents the entanglement distribution rate of the repeater chain, P_{click} the double detection probability, R_{sift} the sifting ratio (assumed equal to 1 in our asymmetric and asymptotic protocol) and r_{∞}^{BB84} the BB-84 secret fraction:

$$R_{\text{rep}} = \frac{1}{T_0} P_0\ P_{QND}^2\ P_W^2 \left(\frac{2}{3} P_{ES}\ P_R^2\right)^n \tag{2}$$

$$P_{\text{click}} = \eta_d^2 \qquad r_{\infty}^{BB84} = 1 - h(e_Z) - h(e_X)\ . \tag{3}$$

In Eq. (2), the quantity $1/T_0$ represents the intrinsic repetition rate of the repeater architecture. We assume here that the memories used are highly multi-mode [33, 35] (see [22, 27] for additional discussions) so that we can avoid to wait acknowledgement from the adjacent stations that the photons have

been received, before proceeding with the protocol or emptying the memory. This allows us to fix $T_0 = 1/R_s$, with R_s the repetition rate of the source. The memories must have a sufficiently large number of modes to be able to store the signals that are received before the acknowledgement arrives. This number can be estimated [22] as $N_m = \gamma R_s \eta_{\max} P_{QND} P_W \frac{L}{c}$, where $\eta_{\max}$ is the maximum single-photon transmittance during the overpass, P_{QND} is the efficiency of the QND measurement, P_W is the writing efficiency of the quantum memory, $\frac{L}{c}$ is the waiting time if all the local operations are instantaneous and γ is a constant close to 1 [34]. N_m amounts to few thousand modes for the distances analysed in this section, which is a demanding but plausible condition [35]. The memory bandwidth of the chosen QM platform limits the maximum repetition rate, that we fix to 20 MHz for the following simulations [22, 36]. P_0 is the transmittance of the elementary links for the entangled pair, which depends on the scheme under study. We identify with P_0 the average of the link transmittance over one fly-by of the satellite for schemes OG (double downlink) and OO (double inter-satellite link or inter-satellite + downlink). P_R is the reading efficiency of the quantum memory. P_{ES} is the success probability of the single entanglement swapping process (we refer to Sec. 3.1 and [28] for details). The term 2/3 is connected with the average amount of time that one has to wait until entangled pairs in adjacent segments of the repeater chain are successfully generated. It arises due to a commonly employed approximation valid for small P_0, which is always valid in the cases under study (we refer to [37] for further details and the exact solution). In Eq. (3), η_d is the efficiency of the detectors used for the final measurement of the photons. The secret fraction r_∞^{BB84} depends, through the binary entropy $h(p) = -p\log_2(p) - (1-p)\log_2(1-p)$, upon the error rates in the X and Z bases, e_X and e_Z. In our simulations they are estimated tracking the evolution of the state of the entangled pairs throughout the ES process, starting from noisy elementary pairs. In a practical experiment these error rates are the result of the parameter estimation stage, in which the parties make public a small subset of their measurement results and compare them. In our analysis we neglect decoherence in the QMs, even though such long distances would require coherence times of the order of tens of ms. We refer to the Appendix 3.1 for additional discussion.

In the following we assume two-qubit systems and we consider, without loss of generality, an entangled state ρ_{AB} diagonal in the Bell basis

$$\begin{aligned}\rho_{AB} = p_{\phi^+} |\phi^+\rangle\langle\phi^+| + p_{\phi^-} |\phi^-\rangle\langle\phi^-| \\ + p_{\psi^+} |\psi^+\rangle\langle\psi^+| + p_{\psi^-} |\psi^-\rangle\langle\psi^-|\end{aligned} \tag{4}$$

with $p_{\phi^+} + p_{\phi^-} + p_{\psi^+} + p_{\psi^-} = 1$ and the Bell states $|\phi\pm\rangle = (|11\rangle \pm |00\rangle)/\sqrt{2}$ and $|\psi^\pm\rangle = (|10\rangle \pm |01\rangle)/\sqrt{2}$. It is possible to apply appropriate local twirling operations that transform an arbitrary two-qubit quantum state in a Bell diagonal state, without compromising the security of the protocol [38]. This structure of the state simplifies the analysis because it can be shown that starting from two Bell-diagonal pairs, the resulting state after entanglement swapping between two sub-systems is still Bell diagonal and the new coefficients $p'_{\phi^+}, p'_{\phi^-}, p'_{\psi^+}, p'_{\psi^-}$ can be readily computed [28]. Then, the error rates along the X and Z directions can be simply written as

$$e_X = p_{\phi^-} + p_{\psi^-} \quad e_Z = p_{\psi^+} + p_{\psi^-} \ . \tag{5}$$

The Bell-diagonal state received by the adjacent repeater stations is assumed to be, without loss of generality, a depolarized state of fidelity F with respect to $|\phi^+\rangle$

$$\begin{aligned}\rho = \rho^{\text{dep}}(F) = F\,|\phi^+\rangle\langle\phi^+| \\ + \frac{1-F}{3}(|\psi^+\rangle\langle\psi^+| + |\psi^-\rangle\langle\psi^-| + |\phi^-\rangle\langle\phi^-|).\end{aligned} \tag{6}$$

The fidelity F accounts for the initial fidelity of the entanglement sources on the satellites and for the noise model that describes the channel. A depolarized state is a natural choice as it corresponds to a common and generic noise that well suits the problem under study and, moreover, any two-qubit mixed quantum state can be reduced to this form using some (previously mentioned) local twirling operations [39].

In the presence of environmental photons entering the receiver, the probability that the detection was due to a signal photon from the adjacent satellite can be estimated as

$$P_s = \frac{N_s}{N_s + N_n} \ , \tag{7}$$

where N_s represents the number of signal photons per time window that we expect to observe (proportional to the transmittance of the channel) and N_n is the expected number of environmental photons in the same time window. Now, with the assumption that environmental photons are unpolarized and uncorrelated to the signal photons, the final state the repeater stations receive is modelled as a mixture of the initial state sent by the sources ρ_0 with the completely mixed state

$$\rho = P_{s1}P_{s2}\rho_0 + (1 - P_{s1}P_{s2})\frac{\mathbb{I}}{4} \ , \tag{8}$$

where $\mathbb{I}$ is the 4×4 identity matrix and P_{s1} and P_{s2} refer to the receiving telescopes of the adjacent repeater stations.

Introducing the definition of the initial state $\rho_0 = \rho^{\text{dep}}(F_0)$ with the initial fidelity F_0 and writing the completely mixed state in the Bell basis we obtain, after comparison with Eq. (6),

$$F = P_{s1}P_{s2}F_0 + (1 - P_{s1}P_{s2})\frac{1}{4} \,. \tag{9}$$

In Sec. 3.1 we show how to estimate the probabilities P_{s1} and P_{s2} in the different cases and which are the most important sources of environmental photons. The fibre-based implementation is substantially immune to this problem and we neglected further sources of error like basis misalignment, so the state that the repeater stations received is actually ρ_0.

We point out that no entanglement distillation [40] is performed in the protocol analysed here. If high quality gates for the implementation of entanglement distillation are available, this operation may allow to get higher key rates and reduce the threshold on the initial fidelity of the pairs and the noise filtering.

Now we discuss the results of the comparison between scheme OO and the other configurations. The parameters employed for the simulations are given in Tab. 1 of the Appendix section. In particular, for schemes OO and OG, we assume the radii of the main optical elements to be 25 cm for the emitters (source satellites) and 50 cm for the receivers (repeater satellites and ground stations). The transmittance of the free-space links is estimated assuming an imperfect Gaussian beam and a simple model for the atmospheric extinction (more details in Sec. 3.2). Regarding detector and quantum memory efficiencies, we assumed rather conservative values, that either have already been achieved separately in different implementations or are expected to be reached in the near future [22]. We also assume that all the satellites are in Earth's shadow and the ground stations are at local night (details about the orbital configurations to achieve this condition are examined in Sec. 1.3). We consider full Moon condition for the estimation of the environmental light (3.1 for details). An important aspect to point out is that in these simulations we consider the satellites passing exactly over the ground stations. In practice most passes will not be close to zenith and a more detailed analysis is necessary. The newly proposed scheme OO will, generally, be more resilient than scheme OG to this problem, since in the latter every link in the chain will be affected, depending on the relative position of satellites and ground stations.

In Fig. 3 we show the secret key rate, see Eq. (1), as a function of the total distance between the parties for several interesting configurations of schemes OO, GG and OG, in the range $[1000, 18000]$ km.

For this range of distances, maximal ES nesting level $n = 2, 3$ are optimal, because for the chosen values of the parameters $n \geq 4$ gives vanishing key rate. We fix the altitude of the orbits at $h = 500$ km in schemes OO and OG. For the latter, at the cost of introducing additional losses, choosing higher orbits has two positive effects: it allows to cover longer distances avoiding the detrimental effect of grazing angle incidence in the atmosphere and makes the fly-by duration longer (see Sec. 3.2 for details). In scheme OO, instead, going to higher altitudes does not have substantial net positive effects.

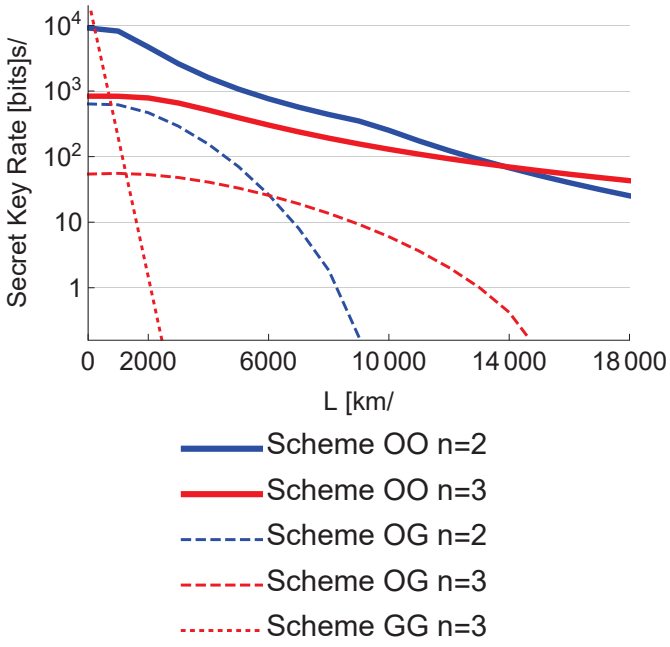

Figure 3: Secret key rate, see Eq. (1), averaged over a fly-by time-window, as a function of the total length of the link for the three schemes analysed in this section. Here, n is the maximal ES nesting level. We refer to Tab. 1 in the Appendix section for details about the choice of parameters.

The use of orbiting quantum repeater stations clearly gives an important boost to the secret key rate, enlarging at the same time the maximum reachable distance, see Fig. 3. Avoiding the effect of the atmosphere allows to truly take advantage of the quadratic scaling of the losses with the distance that characterizes free-space optical channels in vacuum. The proposed scheme OO outperforms schemes GG and OG at every distance beyond $\sim$ 1000 km, by orders of magnitude. In this case, $n = 2$ is enough to achieve non-zero key rate at the longest distance studied. In Fig. 4 we focus instead on shorter distances, in which scheme OO performs again very well. For the satellite implementations $n = 0, 1$ are optimal in this case. With $n = 0$ schemes OO and OG are identical, as there is just a double down-link to the receiving stations of A and B on the ground [19]. In this case, since there are no quantum memories that limit the usable repetition rate, we fix $R_s = 1$ GHz. This

is the source of the advantage at $L < 2000$ km with respect to the other implementations. With $n = 1$, scheme OO beats OG by a factor ~ 10 in this range of distances. These key rates have been derived from the average transmittance during an overpass (P_0). The error rate is also computed from P_0. We checked numerically for some cases the result obtained computing the instantaneous error rate and then averaging it over the pass. The relative difference between the two results is less than 1%.

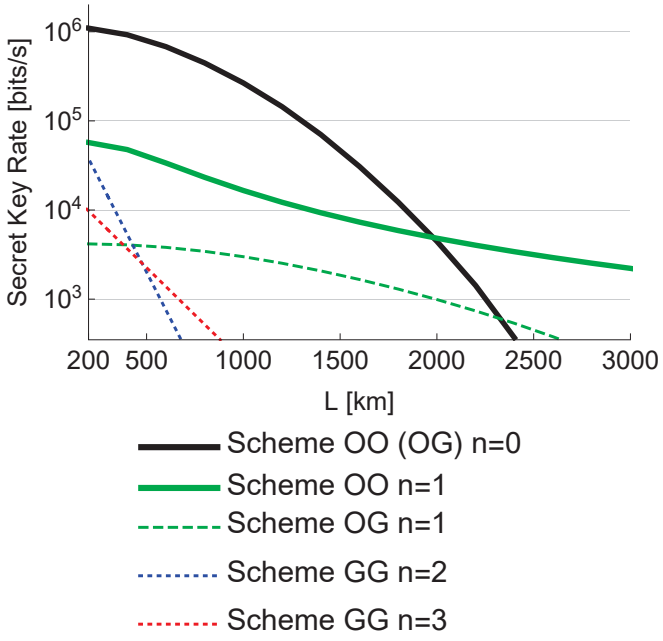

Figure 4: The same considerations as in Fig. 3 apply, but in this case we focus on short-to-medium distances.

It is important to notice that, while for the ground implementation the link is available all day long, the satellite fly-by duration lasts several minutes at most (see Sec. 3.2 for details). Details about the computation of the fly-by duration can be found in the Appendix and the results are shown in Fig. 5. It is evident how, for scheme OG, the fly-by duration goes to 0 when the distance between the ground stations becomes too large, as will be discussed in Sec. 1.2. This is not true for scheme OO, where it only depends on the altitude and it is independent of the distance L for $n \geq 1$.

We study the expected number of secure key bits exchanged in a day in Fig. 6 and Fig. 7. The key rate of Fig. 3 and Fig. 4 has been multiplied by the fly-by duration, considering a single over-pass per day, for schemes OO and OG. In the case of scheme GG we assumed continuous 24h-operation. This comparison, as expected, advantages the ground implementation a bit more, but distances beyond 3000km are still completely impracticable in scheme GG. The advantage of scheme OO over OG gets even bigger, especially at longer distances, since the fly-by duration is longer for scheme OO.

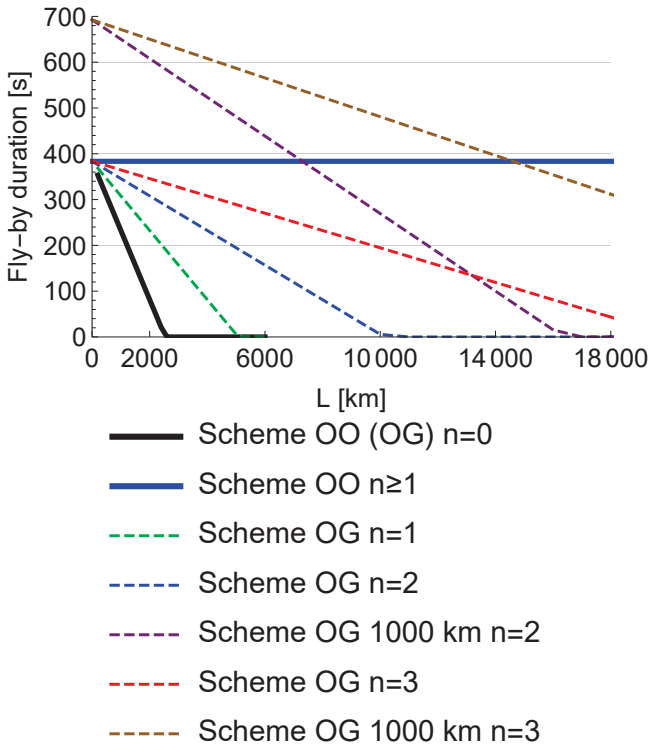

Figure 5: Fly-by duration as a function of the total distance between A and B, for different values of the maximal ES nesting level n and altitude (500km where not specified and 1000km). Notice that for scheme OO the duration is independent of L and $n \geq 1$.

As discussed later in Sec. 1.3, the satellites give coverage to many regions on Earth at every orbit, allowing to operate links between different pairs of users in a single orbit (and there are several orbits in one day). More passes over the same location are also possible, depending on the geography and the orbital configuration. The results shown in Fig. 6 and Fig. 7, that assume one pass per day, are therefore underestimating the actual key exchange per day in many cases, especially at short distances. In other cases, however, one usable pass per day might not be guaranteed, especially when the distance between the parties becomes so large that they are simultaneously at night only for short periods of time. So, we overestimate the average key per day in Fig. 6 for long distances. The deployment of a more complex constellation based on this setup will ease the problem.

Finite size effects can be very significant for satellite-based QKD due to limited satellite overpass duration, leading to small blocks and large statistical uncertainties. If we set a threshold to 30% of the asymptotic value as a satisfactory efficiency, we need a block length of at least $\sim 10^5$ [41]. We then assume the use of $\sim 10^6$ coincident counts at the end nodes to have ample margin for the bits lost during sifting and parameter estimation. This requirement can be met in a single fly-by for distances up to approximately $L \sim 6000$km by scheme OO. This means that for longer distances more overpasses need to be

combined and processed together to avoid the loss of precious secure bits. Even more overpasses need to be combined to achieve the requirement with scheme OG. For scheme GG several days of collection time will be necessary already for distances $L > 2000$km.

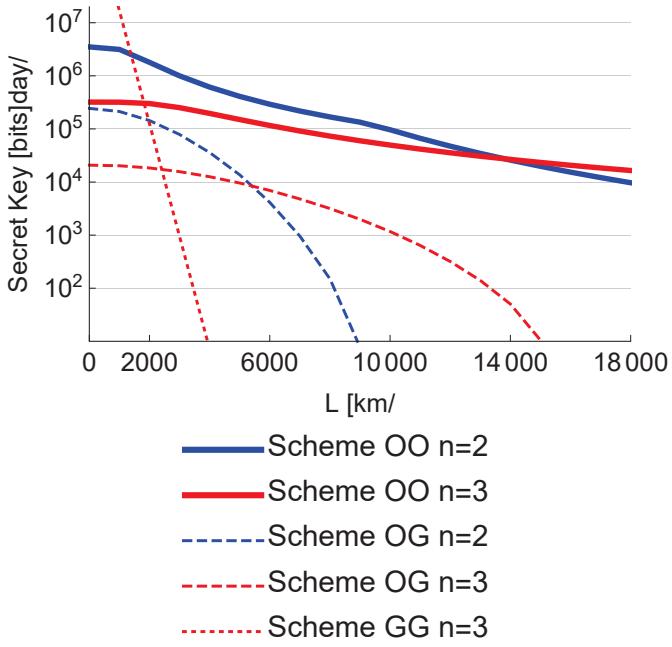

Figure 6: Secret key bits exchanged in 24 hours as a function of the total length of the link for the three schemes analysed in this section. Here, n is the maximal ES nesting level. We refer to Tab. 1 in the Appendix section for details about the choice of parameters.

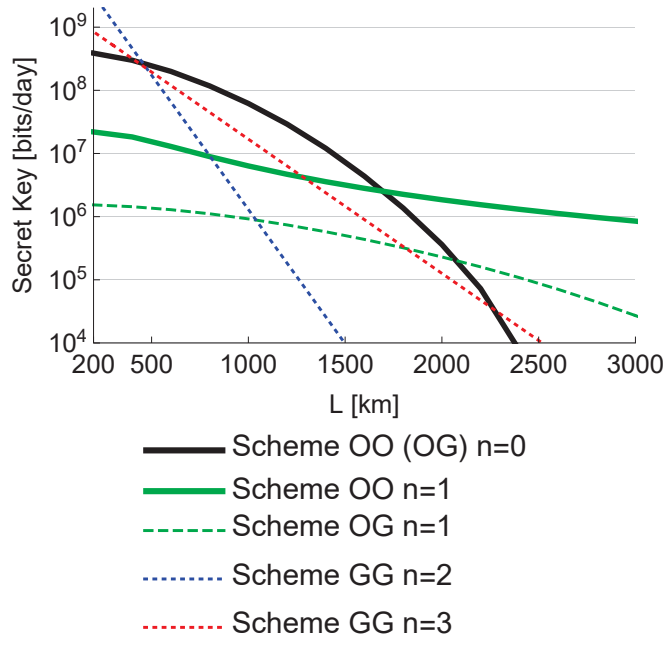

Figure 7: The same considerations as in Fig. 6 apply, but in this case we focus on short-to-medium distances.

We point out that unlike schemes GG and OG, in scheme OO we find links with different transmittance along the repeater chain, in particular double inter-satellite links and twice an inter-satellite + down-link. The bottleneck given by the link with the lowest transmittance determines the overall entanglement distribution rate. For this reason, some parameters need to be fixed in a smart way. For short distances, the inter-satellite links have high transmittance, so the bottle neck is given by the down-links. In this case, increasing the size of the optics on the repeater satellites is not helpful. For longer distances, instead, the inter-satellite links become longer and lossier, so enlarging the correspondent optics allows to improve the bottleneck.

1.2 Pros and cons of orbiting quantum repeater stations

We showed in the previous section how scheme OO of Fig. 1 reaches the highest key rate in many situations of interest. In this section we will list several additional advantages of this configuration over the other two and discuss some of the technical advancements necessary for its deployment.

First of all, it takes full advantage of inter-satellite-links, which allow to completely avoid the degrading effect of the atmosphere. Even if for down-links the additional diffraction and beam deflections introduced by the atmosphere are generally small [21, 23, 24], the inevitable losses due to absorption and backscattering in the air amount to 5-10 dB. In scheme OG, in order for all the links to be active at the same time, good weather conditions must hold in all the intermediate repeater stations. This problem is almost completely solved by scheme OO, for which only the geographical sites of the two parties need to have clear sky conditions. If the channel is divided in 2^n elementary links, clear sky conditions must hold in all the $2^n + 1$ sites on the ground (A, B and the intermediate repeater stations) for scheme OG. Let us assume that the probability of clear sky in all the locations is p_{cs} (uniform and independent). In USA, for example, the sunniest city has $p_{\text{cs}} \simeq 0.7$ [42], so we assume this value as worst-case scenario for scheme OO when compared with OG. In this case, for $n = 3$, scheme OO gives an additional advantage over scheme OG equal to $p_{\text{cs}}^{-(2^n+1-2)} \simeq 12$. The assumption of no correlation in the spatial distribution of cloud coverage is clearly incorrect over short distances. However, the correlation factor generally decreases exponentially with the distance [43] and becomes small (~ 0.2) at around 500km, making our brief analysis reasonable for $L > 4000$km. When one is interested in intercontinental communication, in many cases scheme OG becomes practically unusable, since it would require optical ground stations in the middle of the ocean. The fact that, in scheme OO, all the components apart from the parties' stations are orbiting gives it the advantage. If we analyse Fig.1, we see that in scheme OO the satellites need to communicate with a single ground station at

a time, unlike scheme OG. For this reason, the fly-by time, that corresponds to the maximum time over which exchange of quantum information is possible, is much longer in scheme OO and independent of the distance between the parties (see Fig. 5 in Sec. 1.1 for details). Finally, while in scheme OO the system is able to link only one pair of parties at a time, the chain of satellites can cover the entire world, depending on the choice of the orbit. In this way, a small number of satellites can potentially establish world-wide entanglement distribution, as discussed more thoroughly in Sec. 1.3.

The implementation of a full-fledged quantum repeater on a satellite introduces several additional technical challenges with respect to the other schemes. QM technology is still under development and an architecture ensuring high efficiency, long coherence times and multi-mode functionality is still to be found. However, some of the main necessary technologies have been already individually developed and in some cases tested in the space environment. Needless to say, the implementation of all of them on a single platform will prove difficult and expensive. The low temperature usually needed for the operation of a quantum memory has already been achieved in different experiments. Sub-nK temperatures are expected to be achieved in a trapped atom experiment onboard the International Space Station [44, 45]. The same experiment also tests the ability to reach ultra high vacuum, stable operation of lasers and microwave-radio sources and sizeable artificial magnetic fields. Dilution refrigerators have been implemented already in micro-gravity conditions [46] but solutions with long life-time are still in development [47, 48]. With temperatures around 50mK they would meet the requirements of, for example, quantum memories based on silicon vacancy centres in diamond [36, 49]. The first stages of the refrigerator, at $\sim$ 1K, can also be shared with Superconducting Nanowire Single-Photon Detectors (SNSPDs).

It should be noted that even without considering the quantum devices, the satellites required will be expensive and technically challenging to develop. The choice of 50cm radius telescopes on the repeater satellites, made to have a fair comparison with the OG scheme in terms of parameters, is beyond standard for satellite optical communication. Consider, however, that only the two final satellites of the chain need to independently steer the two telescopes considerably. In scheme OO the middle satellites (including all the repeater satellites) have to point at the adjacent ones, which occupy always the same relative position, requiring very limited steering, that simplifies the design of the satellites. Using smaller receiver telescopes (e.g. 25cm radius) the comparison between the satellite-based schemes will not change and the configuration proposed here will still outperform the fibre-based implementation for a wide range of distances. A more detailed analysis is necessary to assess the cost and the engineering feasibility of satellites with such large independently steerable telescopes. The pointing precision necessary for coupling into single-mode fibre at the receiver is also unprecedented on such platforms.

Optical inter-satellite links, like the ones used in scheme OO, have already been experimentally realized (e.g., during the SILEX mission of the European Space Agency [50, 51, 52]). However, the size of the optical elements, the independent steerability and the pointing precision required will introduce challenges that require further investigation.

In scheme OG the quantum repeater components on the ground could easily be updated over time with newer technology, which is clearly unfeasible in scheme OO. However, we point out that the life-time of LEO satellites is quite short, few tens of years at most, making it necessary to update the hardware in any case.

1.3 Analysis of possible orbital configurations

In this section we qualitatively analyse several types of orbits that may be useful for long-distance entanglement distribution and exemplify the potential of the satellite-based scheme we proposed before. Many recent works analysed the optimal satellite constellations for quantum communication with different protocols [25, 26]. We will focus, instead, on simple configurations of few satellites, to highlight the different possibilities, that can then be used for larger setups.

The 3 different orbital configurations that we are going to analyse are represented schematically in Fig. 8.

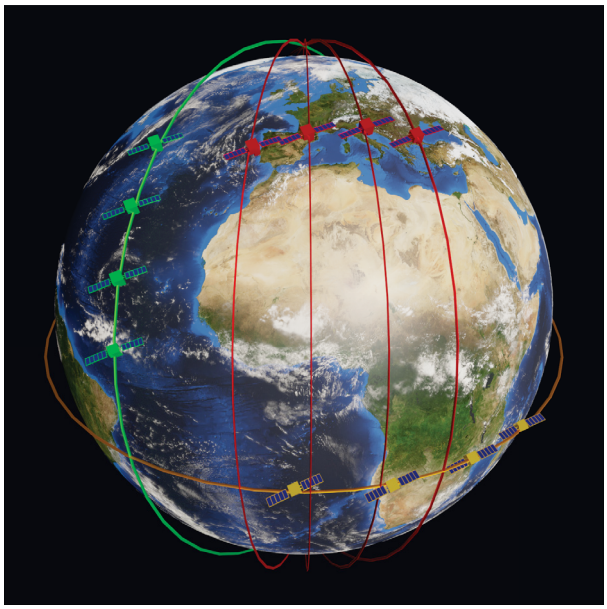

Figure 8: Schematical representation of the orbital configurations analysed in the main text. Sun and Earth synchronous orbits for north-south (east-west) links in green (red), non-polar orbits for east-west links in yellow.

The first example consists in Sun and Earth synchronous orbits, almost polar low Earth orbits that are engineered to pass over a given location always at the same time of the day. These orbits have already been extensively used for all kinds of satellites, from basic research to Earth imaging and proposals for quantum satellite constellations [53]. In order to achieve Earth and Sun synchronism, specific altitude and orbit inclination choices and a propulsion orbit station-keeping system are mandatory. Using such orbital configuration, if we assume that the satellites move one after the other in the already mentioned string of pearls configuration, scheme OO allows to connect parties on the ground in the north-south direction (in green in Fig.8). One can, on the other hand, imagine to put satellites on equidistant Sun and Earth synchronous orbits, forming an arc, as shown in red in Fig. 8. This configuration is very convenient since it allows east-west links with the considerable advantages of Sun and Earth synchronous orbits. In this way we can ensure that the entire satellite chain passes over the target pairs of parties consistently. In order to achieve communication in the east-west direction with the string of pearls configuration one can also use circular orbits with suitable inclination with respect to the equatorial plane (yellow trajectory in Fig. 8), the most promising ones being between 0° and 50°. Such orbits can link locations in the temperate, subtropical and equatorial regions which have roughly the same latitude. If the orbital plane is not actively rotated, the satellite chain will be in a different position at night depending on the time of the year. More satellite chains could be deployed on rotated orbital planes to achieve year-round coverage. This problem does not arise if the orbits are right above the equator. In this case, every pair of users will have several usable fly-bys every night, year-round.

One might be interested in establishing links between different pairs of parties with a single satellite chain. In this case, the number of elementary links 2^n, their length and the orbital configuration need to be optimized depending on the set of locations.

2 Discussion

In this paper we presented a scheme based on the integration between satellite-based optical links and quantum repeaters to achieve long-distance entanglement distribution and untrusted-node quantum key distribution. Several LEO satellites, carrying quantum sources and quantum repeaters, are linked together by means of inter-satellite optical channels. The end-points of the chain are instead linked to two parties on the ground by downlinks. We carefully analyse the repeater rate of the chain and the fidelity of the final shared states, taking into account the effect of different sources of noise. In the end, we compute the asymptotic secret key rate achievable using the BB-84 cryptographic protocol. The parameters used in the simulations have been fixed to reasonably conservative values, that should be achievable in the mid-term future. The asymptotic key rate is compared with the rate achievable by an equivalent fibre-based implementation and a different satellite-based configuration [22], showing that the proposed scheme significantly outperforms the other approaches for a wide range of distances. These results potentially make it a promising candidate building block for a global quantum network, but additional studies are required to examine the feasibility, cost and actual performance in concrete implementations. Our analysis highlights how for this conservative choice of memory parameters and fidelity the satellite-based configurations with maximal nesting level $n = 2$ look more promising than $n = 3$ for mid-term implementation. For better memories and sources the additional round of entanglement swapping would be less costly and the reduced losses in the elementary pairs would allow for higher rates. QM architectures with satisfactory performance in all the fields (efficiency, coherence times, multi-mode capability) are still in the development stage and won't be available for use in the field for many years. However, once such technology will be consolidated, the implementation into satellites seams, in principle, feasible, since many of the technical requirements have been already accomplished in-orbit, as discussed in Sec. 1.2. The design of such platforms, though, will still be very challenging.

The study of quantum-memory-assisted satellite communication has flourished recently [25, 26, 27, 54]. In reference [25] the authors focus on a near-future solution based on a constellation of quantum satellites that operate as trusted nodes. The ability to share entanglement and perform untrusted-node QKD differentiate our findings from theirs. Reference [26] offers a very detailed study of the protocol in [22] in case of a full satellite constellation based on polar orbits, including the optimization of the orbital parameters for a set of major cities around the world. In [27] the authors consider an architecture similar to the one studied here, they analyse pros and cons of different quantum memory platforms and also examine the potential of satellite-based memory-assisted measurement device independent QKD. However, they do not discuss the optimal maximal nesting level n for entanglement swapping, depending on the target distance. Also, the problem of finding useful orbital configurations for the satellite chain is not addressed. In [54] the authors focus on 1- and 2-satellite configurations and analyse the robustness of teleportation protocols, but do not discuss practical implementations.

In summary, the global quantum channels analysed in this work, built through the integration of satellite-based links and repeater nodes, can be envisaged to represent a candidate building block for the future Quantum Internet [55, 56, 57, 58, 59].

3 Appendix

3.1 Error model and environmental photons

In this section we will discuss additional aspects regarding the noise model used for the simulations of Sec. 1. In order to compute the probabilities P_{s1} and P_{s2} of Eq. (9) we need an estimate of the number of environmental photons per time window at the receiver. In the case of scheme OG all the receivers are on the ground and we can consider the same background light for every site. We assume that the receiving telescope has radius r, field of view Ω_{fov} and that we apply spectral and temporal filtering with widths B_f and Δt. If the artificial light pollution is negligible, the power received by the telescope can be expressed as follows [60]

$$P_{\text{noise}} = H_b \Omega_{\text{fov}} \pi r^2 B_f \ . \tag{10}$$

The parameter H_b is the total brightness of the sky background and it depends on the hour of the day and the weather conditions. From Eq. (10) we derive the number of photons per time window

$$N_{\text{noise}} = \frac{H_b}{h\nu} \Omega_{\text{fov}} \pi a^2 B_f \ \Delta t \ , \tag{11}$$

where h is the Planck constant and ν is the frequency of the background photons. Typical values of the brightness of the sky at the wavelength under study (580nm) are $H_b = 10^{-3}\ W\ \text{m}^{-2}\ \text{sr}\ \mu\text{m}$ during a full-Moon night (this value has been used in the simulations in the main text) and $H_b = 1\ W\ \text{m}^{-2}\ \text{sr}\ \mu\text{m}$ for a clear sky in day-time. We point out here that when L is close to the end of the range studied (18000km) the two end ground stations are at *nautical twilight*, so the assumption used in the simulations of full-Moon night is not valid any more. Much shorter values of Δt than the one used in the simulations (Tab.1) can be chosen to keep the noise under control. Considering the synchronization capability demonstrated by Micius [16], values of $\Delta t \sim 1$ns seem totally viable.

In scheme OO we have receivers on the ground (at the parties A and B) and in LEO. The latter ones are used in inter-satellite links, so they are pointing towards the adjacent satellites, in a direction more or less tangent to the Earth's surface and atmosphere. Due to the narrow field of view, they will receive practically no light reflected or diffused from the Earth and the atmosphere. The background light from celestial objects should be negligible and so should be any reflection coming from the sending satellite [60]. This means that the intermediate repeater nodes will be affected by almost no additional noise and only the photons that are sent towards parties A and B at the two ends of the chain will mix with environmental light. However, in order to simplify the analysis, we assume in the simulations that all the photon pairs have the same noise level as the ones comprising the down-link, getting a lower bound on the final secret key rate. When the end ground stations are near dawn/dusk, however, the satellites might be directly hit by Sun light and the assumption above needs to be reconsidered. We assume that the countermeasures proposed in [61], for example building satellites with low albedo, are enough to tackle the problem, but additional analysis might be required.

Another source of errors is represented by dark counts in the detectors used for the BSM. We assume here the standard linear optics setup for polarization-entanglement, in which the photons read from the memories are let interfere on a beam splitter. The light coming out of the two output ports is then analysed using two polarizing beam splitters and 4 single photon detectors. The different click patterns allow to distinguish two out of the four possible Bell states in input. In this case the success probability of the entanglement swapping procedure P_{ES}, used in Eq. (2) of the main text, can be expressed as [28]

$$P_{ES} = \frac{1}{2}\{[1 - p_{\text{dark}}][\eta_d + 2\ p_{\text{dark}}(1 - \eta_d)]\}^2 \ , \tag{12}$$

where p_{dark} is the detector dark count probability

and η_d their efficiency.

In the main text we considered the imperfections of the quantum memories limited to non-unity writing and reading efficiencies. Decoherence in the memories should be addressed too, especially because very long distances beyond 10000 km correspond to long communication times of tens of ms. As discussed in [22], such long coherence times should be achievable by transferring the optical memory excitations to the ground spin states, for example in systems based on Eu-doped yttrium orthosilicate. Electronic spin states can be transferred to long-lived nuclear spin states in silicon-vacancy centres in diamond. In our simulation, such a modification would correspond to a lower value of the writing efficiency P_W and would act in the same way on the different implementations, not changing the comparison between them.

3.2 Modelling the orbits and the transmittance of the satellite links

In this section we will give some details about the orbit model and how the transmittance of the satellite-based optical links has been computed. We assume circular orbits at altitude h above the ground and that, for simplicity, they lie in the equatorial plane. The ground stations are likewise put along the equator. The results of the paper can be extended to repeater chains in different sites of the globe by using suitable orbits (e.g., Sun and Earth synchronous LEO). The law of motion of the satellites and the relative position with respect to the ground stations have then been computed using simple geometrical considerations and the law of gravitational force, without any relativistic correction. In scheme OG, we define the fly-by as the period of time during which the satellite is in line-of-sight contact with both the adjacent ground stations. To be in contact, we suppose that it must be at an elevation angle, in the local coordinate frame of the ground stations, greater than a threshold that we set to 15° [16]. The duration of the fly-by depends on the altitude of the satellite (that also fixes the angular speed), on the orbital direction (the same or opposite to the rotation of the Earth) and on the distance between the ground stations, fixed by the total distance L and n.

The effect is shown in Fig. 5 of the main text, where one can see how the fly-by duration for scheme OG goes to 0 when the distance between the ground stations becomes too large. This is not true for scheme OO, where it only depends on the altitude and it is independent of the distance L for $n \geq 1$.

Numerical studies suggest that a full optimization that would include trimming the edges of the pass, analogously to [62], would only change the final key by a few percent and for simplicity it is omitted here.

In the remainder of this section we will outline the methodology used to estimate the instantaneous value of the transmittance of the free-space links. The beam effects introduced by the atmosphere [24, 21, 23], like additional beam wandering and broadening, are neglected in this work, as their effect is small compared to the strong geometrical losses due to the intrinsic diffraction. Same holds for losses related to pointing inaccuracy. We assume that the transmitter on the satellite generates a collimated imperfect Gaussian beam with initial beam waist W_0 and quality factor M^2 [63]. The value of the parameter M^2 has been fixed to match the far-field divergence of the imperfect Gaussian beam to the one observed for the mission Micius [16, 17, 18, 19]. If we suppose that smaller values of M^2 can be achieved (better correction of optical aberrations) the value of the transmittance of the free-space links can easily go up of a factor $\{5-10\}$.

The atmosphere introduces losses due to absorption and back-scattering that depend on the elevation angle θ of the source and the frequency of the light. We fix the wavelength $\lambda = 580$ nm, the operating wavelength of Eu-doped yttrium orthosilicate memories [35], also a good compromise considering atmospheric extinction and diffraction.

The beam waist of a collimated imperfect Gaussian beam will broaden during the propagation in vacuum, following the relation [64]

$$W(z) = W_0\sqrt{1+(zM^2/z_R)^2}\ . \tag{13}$$

In the far field limit $z \gg z_R/M^2$, with $z_R = \pi W_0^2/\lambda$ the Rayleigh parameter of the beam with wavelength λ, Eq. (13) is linear in the distance z. Now we compute the integral of the Gaussian intensity distribution at the receiver, with beam waist $W(z=\bar{z})$, inside a circular region with radius R, obtaining

$$\eta_{\rm diffr}(\bar{z}) = 1-\exp\left[-2\frac{R}{W^2(\bar{z})}\right]\ . \tag{14}$$

This corresponds with the transmittance of the imperfect Gaussian beam through the receiving aperture of radius R, when the beam is perfectly aligned and centred. This formula can be directly employed for the inter-satellite links of scheme OO, while we multiply it by the factor $\chi_{\rm ext}(\theta) = \exp[-\beta\sec(\theta)]$ to take into account atmospheric extinction. β depends on the site and the atmospheric condition (see [21] for details).

The instantaneous value of the transmittance of the double link from the source to the adjacent repeater stations is then averaged over the fly-by and this quantity is used in Eq. (2) of the main text, labelled as P_0. Scheme OO contains two types of links, double inter-satellite links and twice an inter-satellite

+ down-link. For every configuration we compare the transmittance of the two types of links and used as P_0 the smaller one, that represents the bottleneck in the chain.

In Tab. 1 we report the values of the most important parameters used in the simulations of Sec. 1.

4 Data availability

The data that support the findings of this study are available from the corresponding author upon reasonable request.

References

[1] N. Gisin and R. Thew. Quantum communication. *Nature Photonics*, 1(3):165–171, 2007.

[2] M. Krenn, M. Malik, T. Scheidl, R. Ursin, and A. Zeilinger. *Quantum Communication with Photons*, pages 455–482. Springer International Publishing, Cham, 2016.

[3] V. Giovannetti, S. Lloyd, and L. Maccone. Advances in quantum metrology. *Nature Photonics*, 5(4):222–229, 2011.

[4] G. Tóth and I. Apellaniz. Quantum metrology from a quantum information science perspective. *Journal of Physics A: Mathematical and Theoretical*, 47(42):424006, oct 2014.

[5] E. T. Khabiboulline, J. Borregaard, K. De Greve, and M. D. Lukin. Optical interferometry with quantum networks. *Phys. Rev. Lett.*, 123:070504, Aug 2019.

[6] R. Van Meter and S. J. Devitt. The path to scalable distributed quantum computing. *Computer*, 49(9):31–42, Sep. 2016.

[7] A. Yimsiriwattana and S. J. Lomonaco Jr. Distributed quantum computing: a distributed Shor algorithm. In Eric Donkor, Andrew R. Pirich, and Howard E. Brandt, editors, *Quantum Information and Computation II*, volume 5436, pages 360 – 372. International Society for Optics and Photonics, SPIE, 2004.

[8] H. J. Briegel, J. I. Cirac, W. Dür, G. Giedke, and P. Zoller. *Quantum Repeaters for Quantum Communication*, pages 147–154. Springer Netherlands, Dordrecht, 1999.

[9] N. Sangouard, C. Simon, H. de Riedmatten, and N. Gisin. Quantum repeaters based on atomic ensembles and linear optics. *Rev. Mod. Phys.*, 83:33–80, Mar 2011.

[10] W. J. Munro, K. Azuma, K. Tamaki, and K. Nemoto. Inside quantum repeaters. *IEEE Journal of Selected Topics in Quantum Electronics*, 21(3):78–90, May 2015.

[11] K. Azuma, K. Tamaki, and H.-K. Lo. All-photonic quantum repeaters. *Nature Communications*, 6:6787 EP –, Apr 2015.

[12] M. Zwerger, A. Pirker, V. Dunjko, H. J. Briegel, and W. Dür. Long-range big quantum-data transmission. *Phys. Rev. Lett.*, 120:030503, Jan 2018.

[13] Z. Su, J. Guan, and L. Li. Efficient quantum repeater with respect to both entanglement-concentration rate and complexity of local operations and classical communication. *Phys. Rev. A*, 97:012325, Jan 2018.

[14] A. I. Lvovsky, B. C. Sanders, and W. Tittel. Optical quantum memory. *Nature Photonics*, 3(12):706–714, 2009.

[15] S. Muralidharan, J. Kim, N. Lütkenhaus, M. D. Lukin, and L. Jiang. Ultrafast and fault-tolerant quantum communication across long distances. *Phys. Rev. Lett.*, 112:250501, Jun 2014.

[16] S.-K. Liao et al. Satellite-to-ground quantum key distribution. *Nature*, 549:43, Aug 2017.

[17] J. Yin et al. Satellite-to-ground entanglement-based quantum key distribution. *Phys. Rev. Lett.*, 119:200501, Nov 2017.

[18] J.-G. Ren et al. Ground-to-satellite quantum teleportation. *Nature*, 549:70 EP –, Aug 2017.

[19] J. Yin et al. Satellite-based entanglement distribution over 1200 kilometers. *Science*, 356(6343):1140–1144, 2017.

[20] C. Bonato, A. Tomaello, V. Da Deppo, G. Naletto, and P. Villoresi. Feasibility of satellite quantum key distribution. *New Journal of Physics*, 11(4):045017, 2009.

[21] J.-P. Bourgoin et al. A comprehensive design and performance analysis of low earth orbit satellite quantum communication. *New Journal of Physics*, 15(2):023006, 2013.

[22] K. Boone et al. Entanglement over global distances via quantum repeaters with satellite links. *Phys. Rev. A*, 91:052325, 2015.

[23] R. Bedington, J. M. Arrazola, and A. Ling. Progress in satellite quantum key distribution. *npj Quantum Information*, 3(1):30, 2017.

[24] C. Liorni, H. Kampermann, and D. Bruß. Satellite-based links for quantum key distribution: beam effects and weather dependence. *New Journal of Physics*, 21(9):093055, 2019.

[25] T. Vergoossen, S. Loarte, R. Bedington, H. Kuiper, and A. Ling. Satellite constellations for trusted node QKD networks. arXiv:1903.07845, Mar 2019.

[26] S. Khatri et al. Spooky action at a global distance: analysis of space-based entanglement distribution for the quantum internet. *npj Quantum Information*, 7:4, 2021.

[27] M. Gündoğan et al. Space-borne quantum memories for global quantum communication. arXiv:2006.10636, 2020.

[28] S. Abruzzo et al. Quantum repeaters and quantum key distribution: Analysis of secret-key rates. *Phys. Rev. A*, 87:052315, 2013.

[29] H.-J. Briegel, W. Dür, J. I. Cirac and P. Zoller. Quantum repeaters: The role of imperfect local operations in quantum communication. *Phys. Rev. Lett.*, 81:5932–5935, 1998.

[30] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore*, pages 175–179, 1984.

[31] H.-K. Lo, H. F. Chau, and M. Ardehali Efficient quantum key distribution scheme and proof of its unconditional security *J. of Crypt.*, vol 18, p. 133, 2005.

[32] C. H. Bennett, G. Brassard. and N. D. Mermin Quantum cryptography without Bell's theorem *Phys. Rev. Lett.*, 68, 557, 1992.

[33] H. de Riedmatten, M. Afzelius, M. U. Staudt, C. Simon, and N. Gisin. A solid-state light-matter interface at the single-photon level. *Nature*, 456(7223):773–777, 2008.

[34] If N_p is the expected number of photons received for a given transmittance, the fluctuations will be of order $O[N_p^{1/2}]$. This means that we can choose $\gamma = 1 + O[N_p^{-1/2}]$, which is very close to one since $N_p \gg 1$.

[35] M. Afzelius, C. Simon, H. de Riedmatten, and N. Gisin. Multimode quantum memory based on atomic frequency combs. *Phys. Rev. A*, 79:052329, May 2009.

[36] M. K. Bhaskar et al. Experimental demonstration of memory-enhanced quantum communication. arXiv:1909.01323, 2019.

[37] N. K. Bernardes, L. Praxmeyer, and P. van Loock. Rate analysis for a hybrid quantum repeater. *Phys. Rev. A*, 83:012323, Jan 2011.

[38] R. Renner, N. Gisin, and B. Kraus. Information-theoretic security proof for quantum-key-distribution protocols. *Phys. Rev. A*, 72:012332, Jul 2005.

[39] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters. Mixed-state entanglement and quantum error correction. *Phys. Rev. A*, 54:3824–3851, Nov 1996.

[40] C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher. Concentrating partial entanglement by local operations. *Phys. Rev. A*, 53:2046–2052, Apr 1996.

[41] M. Tomamichel et al. Tight finite-key analysis for quantum cryptography. *Nature Communications*, 3:634, 2012.

[42] Comparative climatic data for the united states through 2018. https://www.ncdc.noaa.gov/ghcn/comparative-climatic-data. Accessed: 2020-03-04.

[43] P. A. Jones. Cloud-Cover Distributions and Correlations. *Journal of Applied Meteorology and Climatology*, 31:7, 1992.

[44] E. R. Elliott et al. Nasa's cold atom lab (cal): system development and ground test status. *npj Microgravity*, 4(1):16, 2018.

[45] T. Schuldt et al. Design of a dual species atom interferometer for space. *Experimental Astronomy*, 39(2):167–206, Jun 2015.

[46] S. Triqueneaux, L. Sentis, P. Camus, A. Benoit, and G. Guyot. Design and performance of the dilution cooler system for the Planck mission. *Cryogenics*, 46(4):288 – 297, 2006.

[47] G. Chaudhry, A. Volpe, P. Camus, S. Triqueneaux, and G. Vermeulen. A closed-cycle dilution refrigerator for space applications. *Cryogenics*, 52:471–477, 10 2012.

[48] M. Zheng et al. A brief review of dilution refrigerator development for space applications. *Journal of Low Temperature Physics*, 197(1):1–9, Oct 2019.

[49] C. T. Nguyen et al. Quantum network nodes based on diamond qubits with an efficient nanophotonic interface. *Phys. Rev. Lett.*, 123:183602, Oct 2019.

[50] G. D. Fletcher, T. R. Hicks, and B. Laurent. The silex optical interorbit link experiment. *Electronics Communication Engineering Journal*, 3(6):273–279, 1991.

[51] G. Planche and V. Chorvalli. SILEX in-orbit performances. *Proceedings of the 5th International Conference on Space Optics*, 2004.

[52] B. Laurent and G. Planche and C. Michel. Intersatellite optical communications: from SILEX to next generation systems. *Proc. SPIE 10568, International Conference on Space Optics*, ICSO 2004, 2018.

[53] L. Mattarella et al. QUARC: Quantum Research Cubesat—A Constellation for Quantum Communication. *Cryptography*, 4(1), 7, 2020.

[54] S. S. Iyengar and M. Mastriani. Satellite quantum repeaters for a quantum Internet. arXiv:2005.03450, 2020.

[55] S. Wehner, D. Elkouss, and R. Hanson. Quantum internet: A vision for the road ahead. *Science*, 362(6412), 2018.

[56] S. Wengerowsky et al. An entanglement-based wavelength-multiplexed quantum communication network. *Nature*, 564(7735):225–228, 2018.

[57] A. Dahlberg et al. A Link Layer Protocol for Quantum Networks. arXiv:1903.09778, Mar 2019.

[58] M. Pant, H. Krovi, D. Towsley, L. Tassiulas, L. Jiang, P. Basu, D. Englund, and S. Guha. Routing entanglement in the quantum internet. *npj Quantum Information*, 5(1):25, 2019.

[59] S. Brito, A. Canabarro, R. Chaves, and D. Cavalcanti. Statistical Properties of the Quantum Internet. *Phys. Rev. Lett.*, 124, 210501, 2020.

[60] E.-L. Miao, Z.-F. Han, S.-S. Gong, T. Zhang, D.-S. Diao, and G.-C. Guo. Background noise of satellite-to-ground quantum key distribution. *New Journal of Physics*, 7(1):215, 2005.

[61] C. Walker et al. Impact of Satellite Constellations on Optical Astronomy and Recommendations Toward Mitigations. *Bulletin of the AAS*, 52(2), 2020

[62] J. S. Sidhu et al. Finite key effects in satellite quantum key distribution. *arXiv*, 2012.07829, 2020

[63] A. E. Siegman. Defining, measuring, and optimizing laser beam quality. In Anup Bhowmik, editor, *Laser Resonators and Coherent Optics: Modeling, Technology, and Applications*, volume 1868, pages 2 – 12. International Society for Optics and Photonics, SPIE, 1993.

[64] B. E. A. Saleh and M. C. Teich. *Fundamentals of photonics*. Wiley series in pure and applied optics. Wiley, 1991.

[65] A. E. Lita, A. J. Miller, and S. W. Nam. Counting near-infrared single-photons with 95% efficiency. *Opt. Express*, 16(5):3032–3040, Mar 2008.

[66] D. Fukuda et al. Titanium-based transition-edge photon number resolving detector with 98% detection efficiency with index-matched small-gap fiber coupling. *Opt. Express*, 19(2):870–875, Jan 2011.

[67] J. Guo. High-performance raman quantum memory with optimal control in room temperature atoms. *Nature Communications*, 10(1):148, 2019.

[68] T. T. Tran et al. Nanodiamonds with photostable, sub-gigahertz linewidth quantum emitters. *APL Photonics*, 2(11):116103, 2017.

5 Acknowledgements

This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No. 675662. D.B. and H.K. acknowledge support from the Federal Ministry of Education and Research BMBF (Project Q.Link.X).

6 Author contributions

C. L. conceived the work and performed the simulations. D. B. and H. K. reviewed the analysis. All the authors discussed the results and contributed to the final manuscript.

7 Competing interests

The authors declare that there are no competing interests.

Parameter	Value	Brief description	Eq./Sec.	Ref.
P_{dark}	10^{-5}	Detector dark click probability	Eq. (12)	[65, 66]
η_d	0.9	Detector efficiency	Eq. (3)	[65, 66]
P_W	0.9	Memory writing efficiency	Eq. (2)	[28, 22, 67]
P_R	0.9	Memory reading efficiency	Eq. (2)	[28, 22, 67]
P_{QND}	0.5	QND measurement efficiency	Eq. (2)	[28, 22, 67]
R_s	20 MHz	Repetition rate of the source	Sec. 1.1	[22, 67]
R_s^{direct}	1 GHz	Repetition rate for direct transmission	Sec. 1.1	[22, 67]
α	0.17 dB/km	Fibre loss coefficient at 1550nm	Sec. 1.1	[28]
W_0	0.25 m	Gaussian beam waist at the transmitter	Eq. (13)	[16, 21, 22]
R_{OO}	0.5 m	Radius receiver telescope, scheme OO	Eq. (14)	[16, 21, 22]
R_{OG}	0.5 m	Radius receiver telescope, scheme OG	Eq. (14)	[16, 21, 22]
λ	580 nm	Wavelength, schemes OO and OG	Sec. 3.2	[22, 35]
M^2	3	Quality factor of the Gaussian beams	Eq. (13)	[16, 63]
β	1.1	Atmospheric extinction parameter at 580nm	Sec. 3.2	[21]
F_0	0.98	Initial pair fidelity	Eq. (9)	[28]
H_b	1.5 $\mu W\text{m}^{-2}$ $\text{sr}^{-1}\text{nm}^{-1}$	Total brightness of the sky background	Eq. (11)	[60, 68]
Ω_{fov}	$(20\ 10^{-6})^2\text{sr}$	Field of view of the receiver	Eq. (11)	[60, 68]
B_f	0.5 nm	Spectral filter bandwidth	Eq. (11)	[60, 68]
ΔT	$1/R_s$	Time filter bandwidth	Eq. (11)	[60, 68]

Table 1: Parameters used in all the simulations in Sec. 1. The parameters have been chosen to represent a reasonable prediction of what can be achieved in the near future. Superconducting Nanowire Single-Photon Detectors (SNSPDs) with low dark count rates and efficiencies exceeding 90% have already been realized at different wavelengths [65, 66]. The quantum memory and heralding parameters have been already used in other theoretical studies [28, 22] and the recent developments in the field make them reasonable [67]. The size of the optical elements imply a significant improvement over previous experiments [16, 17, 18, 19], but qualitatively similar results on the comparison between the schemes can be obtained with smaller optics. The parameters regarding the environmental light filtering should be reasonably easy to achieve and even improve [60, 68].