Design and Optimization of Tools for the Quantum Internet

Raja Yehia

Sorbonne Université - EDITE de Paris

Laboratoire d'Informatique de Sorbonne Université (LIP6) / Quantum Information

Design and Optimization of Tools for the Quantum Internet

Par Raja YEHIA

Thèse de Doctorat d'Informatique

Dirigée par Eleni Diamanti et Iordanis Kerenidis

Présentée et soutenue publiquement en Octobre 2022, devant un jury composé de :

- Alléaume Romain, Professeur à Telecom Paris, Examinateur
- Xuereb André, Professeur à Department of Physics, University of Malta, Rapporteur
- Pappa Anna, Junior group leader à Technische Universität Berlin, Rapporteuse
- Chailloux André, Chercheur, INRIA, Examinateur
- Stobinska Magdalena, Professeure à Institute of Informatics, University of Warsaw, Examinatrice
- Diamanti Eleni, Directrice de Recherche au CNRS, Sorbonne Université, Directrice de thèse
- Kerenidis Iordanis, Directeur de Recherche au CNRS, Université de Paris, Directeur de thèse

Introduction

Revolutions of humankind were always preceded by revolutions in communication between human beings. More than 3500 years B.C., we started encoding our emotions and ideas into symbols that we called writing. It allowed transmission of information beyond generations. The invention of printing around 1450 popularized writing and made it accessible to the masses. There is no doubt that these two events had a tremendous impact on human civilization. Communications have recently reached a new phase with the emergence of communication networks such as the Internet. By encoding information into 0s and 1s and constructing layers of compilers to process it into hardware such as transistors and cables, we are now able to transmit information quasi-instantaneously between two points of the Earth. We are only witnessing the dawn of the revolution it will imply on our civilization. Yet we are already preparing the next phase in information transmission, this time again making use of one of the most recent technologies that we mastered: quantum information.

Quantum Information consists in encoding data into quantum mechanical systems, such as an atom or a photon. Particles indeed have features that cannot be reproduced at our scale. Even if we do not fully understand why particles are behaving this way, we have understood and found methods to exploit their properties to our advantage. Since the discovery of quantum mechanics in the mid-1920s by Niels Bohr, Erwin Schrödinger, Werner Heisenberg, Max Born, Paul Dirac and others, we have found many interesting applications going beyond what we can perform with classical systems. Quantum information can speed up tasks in computation, enhance the precision of our measurements, give better security properties and move the frontiers of what we can achieve in complex systems simulations. The full range of these quantum information applications is not known yet. In this thesis we focus on quantum communications and more particularly in the establishment of a global quantum network called the quantum Internet.

The quantum Internet promises are numerous: it should enhance current classical networking capabilities and allow some new functionalities beyond what is achievable with today's world wide web capabilities. It should help with the design of synchronized clock networks and push current boundaries in metrology. It should allow secure delegation of computation to distant machines, private electronic voting, unforgeability of money and many more interesting applications that will have an impact on our daily lives. The range of these new applications is still to discover and it will undoubtedly lead to groundbreaking changes for our civilisation. Who could have predicted that we would be able to watch movies, order food, access journals and create social networks when the first classical networks were established in the 60s ?

There are however many obstacles towards the establishment of a large scale quantum network. Quantum devices are still at a relatively early stage of development and do not meet yet the requirements to create long distance quantum communication links or store quantum information for a long time. Research communities are organizing to construct standards for quantum communications that will help with the design of efficient hardware and network architectures. Experimentalists and theoreticians are joining their efforts to understand what functionalities can be done as of today through simulations and implement them in real-life scenarios. The quantum Internet community is very active and growing. The tasks are now well defined and researchers can focus on finding near-term or long-term applications, on hardware optimization or construction, or on establishing long-distance communication routines.

This thesis is written in the context of quantum Internet development. We try here to contribute to the community by discussing some security concerns and by providing detailed models and simulation studies of quantum internet architectures and protocols. We also try to give a comprehensive introduction to the quantum Internet that encompasses some of its most important aspects. It hopefully highlights important parameters and issues to resolve, while showing what could be realisable as of today.

The thesis is organised as follows: in Chapter 1 we first introduce the necessary elements of quantum information for the rest of the thesis. We also introduce some notions of classical networking and define the goals and challenges of the quantum Internet. In Chapter 2, we expand on some examples of quantum Internet functionalities and protocols, first focusing on bipartite applications and then on multipartite applications. Then in Chapter 3, we take an abstract step back and examine specific security properties of a protocol that is used as a building block in many other protocols. In the rest of the thesis, we model and simulate different communication settings in order to optimize the protocols and find the best architectures to go forward. In Chapter 4, we expand on long-distance communication between two parties using NV centers as basic node hardware and performing so-called quantum repeater protocols. We investigate different strategies and analyze the effect of imposing a maximal number of attempts on the quality of the quantum link. In Chapter 5, we design a metropolitan quantum network architecture, the Quantum City, whose goal is to be realisable as soon as possible while being scalable, adaptable to future developments and minimizing hardware cost for end users. We also model and simulate different protocols in the Quantum City to get a better idea of what could be achievable as of today. Finally, in Chapter 6, we explore long-distance quantum communication and more particularly satellite-based communication. We design and model communication scenarios between two Quantum Cities separated by hundreds of kilometers. We perform simulations of a few use cases of interest, with today's capabilities.

Table of Contents

Chapter 1

Introduction

For over a century, we have been puzzled by the non-intuitive properties of quantum mechanics. Macroscopic systems have fixed properties and their evolution in time and space can be precisely computed given their initial conditions. When we start looking at systems at the quantum scale, typically the size of a photon or an atom, we see that they behave differently. Particles have wavelike features that can be described using the Schrödinger equation. As a consequence, their properties, such as their position or their spin at a specific time, are not fixed but rather probabilistic. They can be in superposition of different values or share correlations that can not be explained with classical theory. Even more strange, when we measure these particle features, they are fixed to a specific value. These surprising and sometimes counter intuitive properties are still an enigma for many scientists but their mathematical description is now well known. In fact, we know them so well that we can use them to encode and process information with particles to achieve capabilities beyond what is possible with classical systems. The range of these new applications is still unknown. More and more exciting possibilities arise as our control on quantum systems grows.

One area where encoding information in quantum systems enhances today's capabilities is communication, and more particularly communication networks. By creating large networks of distant quantum devices and allowing them to exchange quantum data, we can envision several enhancements to today's classical Internet that should impact our daily lives.

Outline: In this chapter, we introduce elements of quantum information theory and classical network theory that we will use throughout this thesis. We first recall, in Sec. 1.1, the basics of quantum information such as single-qubit and multi-qubit systems as well as some common operations on them. We also go over a few physical systems that will be used in further chapters of this thesis. Then, in Sec. 1.2, we introduce premises of today's classical communications: the OSI model used in the creation of the classical Internet and some classical security definitions. Finally, in Sec. 1.3, we dive into the main focus of this thesis: quantum networks and the Quantum Internet. We give a definition, highlight the main challenges and present some of the most recent advances.

1.1 Quantum information

1.1.1 Basics of quantum information

Quantum information is a novel way to manipulate information. It uses the fascinating properties of quantum mechanical systems to change the way information is handled at its core by computing devices. Information is no longer encoded in bits but in quantum bits or *qubits*. Qubits aim to represent two-level physical quantum systems such as the polarization of a photon or the spin of an electron. These two levels are represented using the Dirac notation with the so-called ket $|0\rangle$ and $|1\rangle$. Just like bits, qubits are an abstract way to talk about information. In this section, we give a brief introduction to some mathematical definitions and tools in quantum information that will be of use in the rest of this thesis. We refer the interested reader to [1] for more precisions.

In general, pure quantum states are unit vectors in a Hilbert space $\mathcal{H}$ of some dimension. Qubits are pure quantum states of two dimensions, hence they are normalized vectors in a two-dimensional Hilbert space $\mathcal{H}_2$ (see Eq. 1.1). They lie on the surface of a sphere that we call the Bloch Sphere (see Fig. 1.1).

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \tag{1.1}$$

with $|0\rangle = \begin{pmatrix}1\\0\end{pmatrix}$, $|1\rangle = \begin{pmatrix}0\\1\end{pmatrix}$, $(\alpha, \beta) \in \mathbb{C}^2$ and $|\alpha|^2 + |\beta|^2 = 1$. When α or β is equal to 0, then $|\psi\rangle$ is equivalent to a bit in the state 0 or 1. When this is not the case, we say that $|\psi\rangle$ is in superposition of 0 and 1. Superposition is the first major difference between classical bits and qubits. One of the postulates of quantum information is that any qubit in the form of Eq. 1.1 is a valid quantum system. Usual qubit states are $|0\rangle$, $|1\rangle$, $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, the last two representing the equal superposition between $|0\rangle$ and $|1\rangle$.

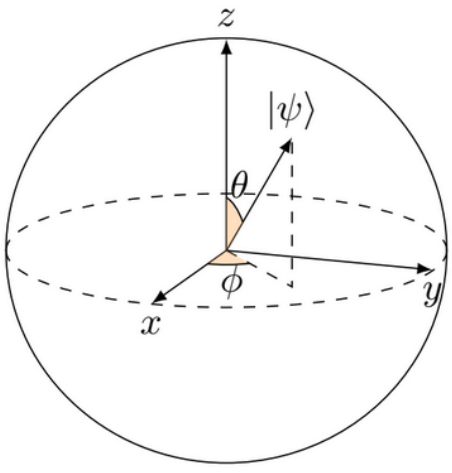


Figure 1.1: Representation of an arbitrary qubit on the Bloch Sphere.

The set $\{|0\rangle, |1\rangle\}$ is a natural basis for the qubit Hilbert space $\mathcal{H}_2$, and we will denote it as the *computational basis*. The set $\{|+\rangle, |-\rangle\}$ is also a basis of $\mathcal{H}_2$ that we denote as the *diagonal basis*.

Qubit manipulation is done through linear unitary trace-preserving matrices that rotate the qubit on the Bloch sphere. In a circuit-based model in which each qubit is modeled by a wire going from left to right, we call these matrices *quantum gates*. Quantum gates are used to manipulate information in order to perform algorithms taking quantum states as input. The usual set of gates that we use to design protocols is represented by the Pauli matrices and the Hadamard matrix:

$$I := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad X := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$
$$Z := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \qquad Y := \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix},$$
$$H := \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

The Pauli-X gate (also called *bit-flip*) is the quantum analog of the classical NOT gate: it takes the $|0\rangle$ state to the $|1\rangle$ state. The Pauli-Z (also called phase-flip), Pauli-Y and Hadamard gates however have no classical analog. The Hadamard gate is the transition matrix between the computational basis and the diagonal basis: it takes the $|0\rangle$ state to the $|+\rangle$ state.

While classical bits can only have two values 0 and 1, qubits can have infinitely many values, namely all the vectors of the form of Eq. 1.1 with norm 1. However, this does not mean that an infinite amount of data can be stored in a qubit. In fact, very little information is accessible for an external observer. The information an observer can extract from a quantum state is defined by the way it is measured. Moreover measuring a quantum system inherently alters it, and sometimes even completely destroys it. This measurement process is another major difference between classical and quantum systems. The interpretation of quantum measurements gives rise to debates in the community, leading to different interpretations of the fundamental nature of quantum systems that we will not detail here.

In general, measurements are defined by a set of measurement operations $\{M_n\}$ that project quantum states on an axis or into a subspace. This set defines a *measurement basis* that determines the possible outcomes of the measurement. Two quantum states prepared identically can yield different measurement outcomes depending on the measurement basis that is chosen. Actually, even for the same measurement basis, the outcome of a measurement is probabilistic. When a measurement is performed on a state $|\psi\rangle$, the probability of getting an outcome n is given by the Born rule (see Eq. 1.2). When this happens, the state is modified as shown in Eq. 1.3.

$$Prob(n, \psi) = \langle\psi| M_n^\dagger M_n |\psi\rangle \tag{1.2}$$

$$|\psi\rangle \xrightarrow{\text{outcome } n} \frac{M_n |\psi\rangle}{\sqrt{\langle\psi| M_n^\dagger M_n |\psi\rangle}} \tag{1.3}$$

For qubit states, usual measurement basis are the computational basis given by $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$ and the diagonal basis $\{|+\rangle\langle +|, |-\rangle\langle -|\}$. As an example, the measurement in the computational basis of a qubit state $|\psi\rangle$ in the form of Eq. 1.1 yields the outcome 0 with probability $|\alpha|^2$ and the outcome 1 with probability $|\beta|^2$. If the outcome is 0, we say that $|\psi\rangle$ *collapses* into the state $|0\rangle$.

In both classical and quantum physics, some objects are defined through statistical mixtures. For example a system can be described with the sentence: *"There is a probability p that the system is in the state A and a probability* $(1-p)$ *that the system is in the state B."*. In quantum physics, we talk about mixed quantum states as opposed to pure quantum states. Mixed quantum states correspond to a statistical mixture of states $|\psi_i\rangle$, each appearing with some probability p_i. The mathematical representation for mixed states is the *density matrix* representation, given by Eq. 1.4. It is a very useful tool in quantum information as the eigenvalues and eigenvectors of a density matrix exhibit important properties of a quantum state. Since quantum states cannot be known before we measure them, mixed states can be a useful representation of the information contained in a system at different steps of a quantum process.

$$\rho := \sum_i p_i |\psi_i\rangle\langle\psi_i| \tag{1.4}$$

The transfer of quantum information is usually defined through *quantum channels*. They are maps that generalize the concept of quantum gates defined above to the context of communication. Generally, quantum channel $\mathcal{N}$ maps a quantum state ρ in some Hilbert space $\mathcal{H}_A$ into another Hilbert space $\mathcal{H}_B$. Since it should preserve the normalization of state, it is a trace-preserving map meaning that $\mathrm{Tr}(\rho) = \mathrm{Tr}(\mathcal{N}(\rho))$. For $\mathcal{N}(\rho)$ to be a valid quantum state, we also require that quantum channels are completely positive maps. As we will see in this thesis, quantum channels are useful for representing loss and noise in quantum operations.

An important property of a quantum system is its *fidelity* with respect to another known system. It is a measure of how close two quantum states are to each other. Fidelity expresses the probability that a state passes a test identifying it as the other. In general, the fidelity of a state $\rho = |\psi_\rho\rangle\langle\psi_\rho|$ with respect to another state $\sigma = |\psi_\sigma\rangle\langle\psi_\sigma|$ is given by the trace of the product of the density matrices: $F(\rho,\sigma) = (\mathrm{tr}\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}})^2$. For pure states, the fidelity reduces to the squared overlap between the state vectors $F(\rho,\sigma) = |\langle\psi_\rho|\psi_\sigma\rangle|^2$. Good fidelity of a physical quantum system with respect to the ideal state that it is expected to represent is a crucial parameter for quantum information processing as we will see in Chap 3.

We have defined some mathematical tools to describe and manipulate a single qubit. Encoding information in a two-level degree of liberty of a quantum system to create single-qubit systems is the basic building block of quantum information processing. However, most interesting phenomena happen where many of these systems are interacting.

1.1.2 Multi-qubit systems

To describe a quantum system with more than one particle we use the *tensor product*. It is a bilinear map $\bigotimes$ going from two Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ of respective dimension m and n to a Hilbert space of dimension $m \times n$ usually denoted $\mathcal{H}_A \bigotimes \mathcal{H}_B$. For example a two-qubit system where the first qubit is in the state $|0\rangle$ and the second in the state $|1\rangle$ is the state $|0\rangle \bigotimes |1\rangle$ that we commonly write $|01\rangle$ for simplicity. The general form of a two-qubit system is given in Eq. 1.5. It lies in the Hilbert space $\mathcal{H}_4 = \mathcal{H}_2 \bigotimes \mathcal{H}_2$ of dimension 4 whose basis is given by the tensor product of the vectors of the basis of each subspace: $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$.

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle \tag{1.5}$$

with $|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$. As in the single qubit state case, these coefficients correspond to the probability of getting each possible outcome, 00, 01, 10 or 11 when simultaneously measuring the two qubits in the computational basis. Two-qubit states can also be written using the density matrix formalism. Each part of the system can then be investigated using the partial trace operation. The partial trace outputs the reduced density matrix, that represents the information one can have given only a part of the system without considering the rest (e.g. only one particle in the case of a two-particles system).

Any state of the form of Eq. 1.5 is a valid quantum state that can be created in a quantum system in the laboratory. When it can be expressed as the tensor product of single qubit states, it is said to be separable. When it cannot, we say that the state is *entangled*. Entanglement is yet another fascinating property of quantum theory that arises with multi-qubit systems. When a state is entangled, the two particles forming it cannot be described independently. Measuring the different parts of an entangled state will give outputs sharing correlations that sometimes cannot be explained with classical theory. Indeed, classical theories based on local hidden variables that explain the correlations between measurements outputs give rise to inequalities such as the famous Bell inequality [2]. Entanglement between two separate systems is a necessary resource to violate a Bell inequality in a test (although the converse is not always true). Experimental results show violation of this inequality in physical systems [3], which demonstrates the existence of entanglement in nature.

Examples of entangled two qubits state are the *Bell state* or *EPR pairs*:

$$|\phi^+\rangle := \frac{|00\rangle + |11\rangle}{\sqrt{2}}, \qquad |\psi^+\rangle := \frac{|01\rangle + |10\rangle}{\sqrt{2}},$$
$$|\phi^-\rangle := \frac{|00\rangle - |11\rangle}{\sqrt{2}}, \qquad |\psi^-\rangle := \frac{|01\rangle - |10\rangle}{\sqrt{2}},$$

These states are useful in many protocols as we will see in the next chapter. They are maximally entangled as the reduced density matrix on either system is maximally mixed. They can also be used as a measurement basis for the joint measure of two qubits. This is called a *Bell State Measurement* (BSM), it projects the state of the two qubits into one of the four Bell states.

Operations on multi-qubit states are also done with unitary matrices. When an operation is done independently on each part of a multi-qubit system, it is described using the tensor product of the unitary matrices that describe each independent operation. For example, applying a bit-flip gate on one qubit of a two-qubit system and doing nothing to the second qubit is described by the matrix $X \otimes I$. However, operations on two-qubits systems can be based on the interaction between the two qubits. A common example of such two qubits operation is the CNOT operation. It corresponds to conditional statement in classical algorithmic: if the first qubit is in the state $|1\rangle$ then the second qubit is flipped, otherwise nothing happens. The CNOT gate entangles the two qubits it is applied to, and it can be found in many protocols and algorithms.

$$\text{CNOT} := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

The construction of the two-qubit system generalizes to quantum states with an arbitrary finite number of qubits. This means that the space of possible quantum states grows exponentially with the number of qubits. For the sake of simplicity we will write the n-qubit state $|0\rangle \bigotimes |0\rangle ... \bigotimes |0\rangle$ as $|0\rangle^{\otimes n}$. Multipartite states can also be entangled when they cannot be expressed as tensor products of subsystems, although the classification of multipartite entangled states is richer than in the bipartite case. In multipartite entanglement, apart from fully separable states and fully entangled states, there also exists the notion of partially separable states [4] which we will not detail in this thesis.

One multipartite entangled state that will be of great importance in this thesis is the Greenberger–Horne–Zeilinger (GHZ) state [5] which, for $n \geq 3$ qubits, is given by Eq. 1.6. It is a necessary resource for many multiparty network protocols. Unfortunately the creation of this state in the laboratory is relatively hard as we will detail in next chapters.

$$|\text{GHZ}_n\rangle := \frac{|0\rangle^{\otimes n} + |1\rangle^{\otimes n}}{\sqrt{2}} \tag{1.6}$$

Finally, an important result in quantum information is the *no-cloning theorem*. It states that it is impossible to create an identical copy of an arbitrary unknown quantum state. It is a direct consequence of the measurement principle: once we measure a quantum system, we modify it and, hence, lose some information about it. As we will see later, it has important consequences on quantum communications and it is a useful tool for the security of quantum protocols. The no-cloning theorem can be proven simply using the following proof: let us imagine a quantum channel $\mathcal{N}$ that copies perfectly a quantum state into another state initially in the state $|0\rangle$, i.e. that for all $|\psi\rangle$ in the form of Eq. 1.1, $\mathcal{N}(|\psi\rangle \otimes |0\rangle) = |\psi\rangle\,|\psi\rangle = \alpha^2\,|00\rangle + \alpha\beta\,|01\rangle + \beta\alpha\,|10\rangle + \beta^2\,|11\rangle$. Then we have that $\mathcal{N}(|0\rangle \otimes |0\rangle) = |0\rangle\,|0\rangle$ and $\mathcal{N}(|1\rangle \otimes |0\rangle) = |1\rangle\,|1\rangle$. Thus, by linearity of the quantum channel, $\mathcal{N}(|\psi\rangle \otimes |0\rangle) = \mathcal{N}(\alpha\,|0\rangle \otimes |0\rangle) + \mathcal{N}(\beta\,|1\rangle \otimes |0\rangle) = \alpha\,|00\rangle + \beta\,|11\rangle$ which is not equal to $|\psi\rangle\,|\psi\rangle$. This proves that it is not possible to construct a valid channel that would copy any arbitrary quantum state.

1.1.3 Physical supports for quantum information

As we mentioned before, quantum information is the encoding and processing of information in quantum systems. One particular issue with quantum objects is that they are subject to a phenomenon called *decoherence*. Quantum objects cannot be completely isolated from their environment, otherwise we could not even manipulate them. Due to their interaction with the environment, quantum objects are known to lose their information with time. This information loss process is called decoherence. Many research efforts are dedicated to creating quantum memories that would be able to maintain the coherence of a quantum state for a long time. It is not yet known which physical support is the most appropriated for large scale quantum information processing. Several physical supports for quantum information are under study by the research community. It is likely that quantum processing devices will work in hybrid mode, with different quantum systems interacting together. Here we give a non-exhaustive list of ways to encode data into quantum systems and detail the ones that will be of use in this thesis.

Photonic qubits are one of the most studied supports for quantum information as they have the non-negligible advantage of being resistant to decoherence. Coding information in a degree of freedom of a particle of light is moreover convenient for transporting this information into optical fibers or free space as we will detail in later chapters of this thesis. The degrees of freedom that are most used in single-photon information processing are the polarization of the photon, its path or its arrival time. Each exhibits quantum properties that have different pros and cons. Creating single photons in practice is done using, for instance, weak laser pulses or a phenomenon called Spontaneous Parametric Down Conversion (SPDC) that we we will detail in Chapter 5. Measurement of single photons is done using chains of reactions involving supraconducting detectors that have very high efficiency but necessitate a cryostat to work. Light pulses can also be used to encode information in the quadratures of its electromagnetic field. This is called Continuous-Variable (CV) encoding of information as the value of the quadratures can be continuous. These quadratures can be accessed using so-called homodyne and heterodyne measurements. We will not detail much on this as we will not be using the CV encoding in this thesis. Photonic qubits are mostly used for communication between distant nodes as for example in [3, 6] but there are also proposals to use them for computation purposes [7].

Qubits can also be encoded in solid-state spin systems such as nytrogen-vacancy (NV) center in a diamond structure (see Fig. 1.2). This defect center is a prime candidate for a quantum communication network due to its packaged combination of a bright optical interface featuring spin-conserving optical transitions that enable high-fidelity single-shot readout [8] and individually addressable, weakly coupled ^{13}C memory qubits that can be used to store quantum states in a robust fashion [9, 10]. Moreover, second-long coherence times of an NV electron spin have been achieved [11]. Specifically, the optical interface of the electron spin allows for the generation of spin-photon entanglement, where the photonic qubits can then be transmitted over large distances. The carbon nuclear spin acts as a long-lived memory, but can be accessed only through the interaction with the electron spin. Information encoded in the electron spin can be swapped to the carbon qubit and joint measurement such as BSM can be done jointly on the two systems. In Chapter 4, we detail how to model the qubits in NV centers and how to use them to perform communication protocols.

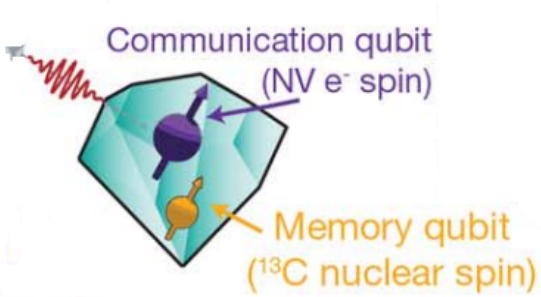


Figure 1.2: Schematic of an NV center in a diamond. It contains two addressable qubits: the spin of an electron with an optical interface coupled to a ^{13}C memory qubit.

Other so-called defect centers can be used in the same way to encode quantum information such as Silicium vacancy centers [12] or rare-earth ions [13]. Ions can be trapped into arrays of individually addressable qubits however there exists some difficulties in scaling up these systems [14]. Atoms can also be used collectively to enhance their interaction with photons in a cavity, thus creating so-called atomic ensemble states that can be used for computation [15] or communication [16]. Other solutions that have gained a lot of visibility due to their performances are semiconductor quantum dots in GaAs system [17] or in Silicon (see [18] for a review). Finally, superconducting qubits that make use of the Josephson junctions are also good candidates for quantum computing devices [19]. This list is of course not exhaustive, but it shows that until now, no standard has emerged on the physical implementation of future quantum devices: there are many different proposals in creating physical qubits. As we will not use them in the rest of this thesis, we will not dive into the details of each of these qubit implementations.

1.2 Classical networks considerations

1.2.1 The OSI model

Since the 1960s, classical networks have flourished and have been optimized to efficiently link any two points on Earth. We can now transfer packets of data from a party to another at a very high speed through the Internet, an international network architecture of servers and computers linked mostly by cables. The Internet has been constructed by increments, to optimize as much as possible the transfer of information. Network protocols have been standardized and are now widely used for data transmission. International organizations have been created such as the Internet Engineering Task Force (IETF) to develop and promote Internet standards.

In 1984, researchers and engineers have created a conceptual model for designing network architectures and hardware: the Open Systems Interconnection (OSI) model. It separates the network into seven layers that we show in Fig. 1.3. It describes a universal standard for communication in a classical network without any regards to the underlying technology. The goal of the OSI model is to facilitate the design of hardware on one side and application on the other side. Indeed, interoperability between different communication systems is crucial for developing new technologies and applications. Nowadays, an engineer can design a new application without having to think or even understand how bits are processed by the hardware.

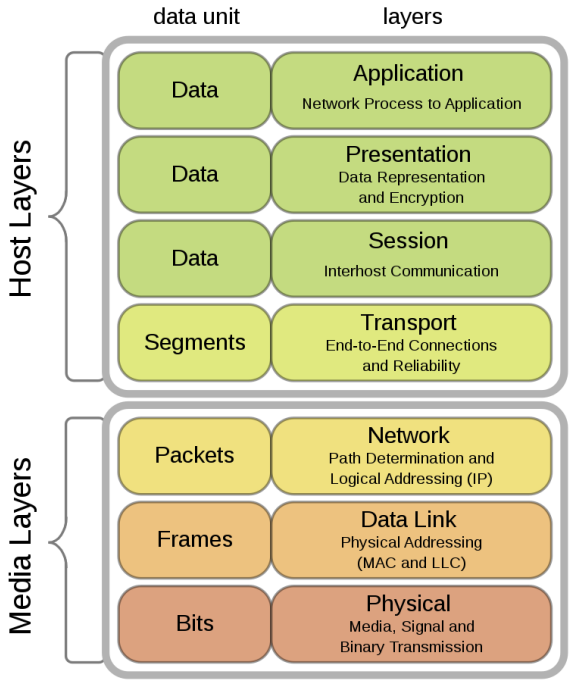


Figure 1.3: The 7 layers of the OSI model that partition the flow of data

The physical layer is responsible for the emission and reception of raw data. It converts bits into electrical, optical or radio signals that are processed by the hardware. The data Link layer provides direct data transfer in a local network and takes care of correcting some error remaining from the physical layer. This is where ethernet lives and where MAC address of every machine is used to route data in local networks. The network layer encapsulates data into packets in which the source and destination addresses are written. This is where routing of the data between distant networks happens and where IP addresses are in play. Then comes the transport layer which takes care of segmenting the data packet and actually transporting it from a local network to another. The session layer establishes, manages and terminates the connections between the local and remote server, and synchronizes different tasks. The presentation layer translates the data into the format required by the application layer. Finally the application layer is the one that is directly used by the end user through a software, such as Web browsers or file explorers.

Whenever a user wants to send or receive data on the Internet, the data flows from layer 7 down to layer 1 from the sender side, and then flows from layer 1 to layer 7 on the receiver device. This process is called encapsulation/decapsulation. It consists in splitting the data into packets and adding headers with the necessary information for routing the packets in the network as well as information about the content. Packets often contain an error-check value that the receiving device can use to confirm the full reception of the packet. There are standard protocols that are used in each layer such as FTP for file transfer, SMTP for emails, HTTP/HTTPS for information transfer on the web and many others. They define organizational rules for the data packets according to the protocols the network supports.

The OSI model is now replaced by the TCP/IP model with four layers. It roughly groups the application, presentation and session layers of the OSI model into one application layer, the physical and data link layers into one physical layer and keeps the network and transport layer. However, the OSI model is still at the core of the design of classical network architectures. It is a useful tool to understand the complexity in designing applications over a very large network. It shows the necessity of breaking down the different processes happening in data transmission and to make them interact in the most standardized way possible. This is a crucial step towards scaling up network architectures.

1.2.2 Secure classical communication

Several applications are already available in the classical Internet, from browsing collaborative websites to multiparty computation. However one crucial application for many users of the classical Internet is secure communication. Private communication between any two users has been the focus of many developers since the dawn of the Internet. Efficient protocols now exist to allow private bipartite communications; however most of them rely on the same first step: to create a shared secret key between two parties. The most simple and secure way to transmit a message is then to apply the logic gate XOR between the key and the message, yielding a completely random cyphertext. This protocol is called the One-Time Pad protocol (see Fig. 1.4).

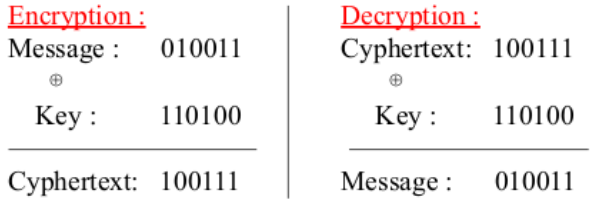


Figure 1.4: One-Time Pad protocol (OTP): the encryption of the message is done by applying a XOR between the key and the message. The cyphertext can then be send to another party. Only a user holding the same key is able to perfectly decrypt the message by applying again a XOR operation.

One can say that creating a shared secret key is key to private communications. The OTP protocol is however quite inefficient as the key can be used only once. Indeed, a repeated use of the same key creates the risk of finding patterns in the cyphertext that would allow a malicious eavesdropper to guess the key. Another downside of the OTP is that the key has to be the same size as the message. Several techniques have been found to reduce the size of the key, such as changing the message into a smaller message using hash functions. In so called *symmetric* protocols, the same key is used for encryption and description and thus must be shared between the two parties, while in *asymmetric* protocols, each user possess a private and a public key. By doing communication rounds, the parties can ensure that the message is always well encrypted when going through classical channels. A large key can also be extracted from a small shared key by using key expansion algorithms.

These processes are now very efficient, sometimes even embedded in the way the processors of our computer store the data. As we will see in the next chapter, quantum encoding of data offers new protocols to create a shared secret key. One point that remains however complicated, even with quantum devices, is *authentication* of the data, i.e. proving the identity of a user of a network. In other words, making sure that the parties involved in the communication are really who they pretend to be still necessitates sharing a small classical key between the two parties. This property is still essential for many quantum network protocols, for example Quantum Key Distribution as we detail in Sec. 2.1.1.5.

The hashing functions and protocols that are used to create a key in the classical Internet rely on *computational security*. This means that the time it would take for an eavesdropper to guess the key using the best available classical computer is too long to be practical. More formally the complexity of solving the problem needed to crack the key grows exponentially with a parameter that the honest senders and receivers control. They thus can make sure that no-one with current technologies can realistically hack their communications.

While being very robust and universally adopted, relying on computational assumption carries the risk of having a new technology discovered that would render the security system useless. For example in 1995, P. Shor discovered a quantum algorithm able to efficiently factorize great numbers into their prime factors [20] which is the primitive of the RSA algorithm, the most widely used security system for data transmission. To this day this result is one of the most impactful results in quantum computation. Fortunately, new post-quantum secure algorithms are being carefully developed to ensure the security of data transmission even if quantum computing becomes accessible to the masses. Post-quantum cryptography protocols still rely on computational security, however, to this day, no efficient classical or quantum algorithm able to crack them have been found.

We point out that the security of a communication is not only defined by the privacy of data transmission. It is usually broken down into three main properties: Confidentiality, Integrity and Availability (CIA). Confidentiality corresponds to the privacy of the transmitted data, while integrity corresponds to unaltered transmitted data. The integrity of the data can be seen as the other side of the coin of data authentication. Finally Availability corresponds to a communication channel that remains accessible despite all attacks. It involves maintaining hardware and technical infrastructure that display the information. Example of attacks against availability are Denial of Service (DoS) attacks, that consist in overflowing a server with malicious requests until it cannot accept honest requests.

1.3 The Quantum Internet

1.3.1 Definition and goals

Various applications have been discovered to make full use of information encoded in quantum states. Among them are applications in quantum computation, quantum metrology, quantum simulations and quantum communication. In this thesis we focus on the latter, and more particularly on quantum networking. It uses the fundamental properties of quantum mechanics that we described before, superposition, entanglement and measurement, to achieve capabilities that are are beyond what is possible with classical networks. Quantum networks allow, for example, the creation of quantum sensor networks that will push the boundaries of current metrology as well as more precise clock synchronization between devices, with applications in the study of gravitational waves [21]. The holy grail of research in quantum networking is the establishment of a full scale quantum Internet that could be used by everyone.

Just as the classical internet is a network of classical devices connected, we can define the Quantum Internet as a global network of quantum devices linked through quantum channels. The objective is to enhance the classical Internet by enabling quantum communication between any two points of the network. The quantum Internet should indeed work in parallel of the classical internet. To help with the design of a standardized architecture like the OSI model from the previous section, a research group has been created at the Internet Engineering Task Force (IETF): the Quantum Internet Research Group (QIRG), whose focus is precisely to address the question of how to design and build quantum networks.

The QIRG has set goals and architectural principles that help the community develop quantum networks. According to these principles, the goal of a Quantum Internet architecture in development should first be to support distributed quantum applications and enhance today's networking ability. But it should also allow for growth and adaptability to tomorrow's applications to avoid changing the whole hardware at each new protocol generation. It should support hardware heterogeneity because many new hardware and techniques are still being investigated and it is not clear what will actually be used. It should be easy to manage and monitor and it should be resilient to failure and malicious actors. More importantly this quantum internet should work as soon as possible. In Chapter 5 we will expand on a model for a metropolitan quantum network that fits these goals.

Entanglement is the fundamental resource of quantum networks. It is possible to use the non-classical correlations that stem from measuring entangled states in order to create completely new types of applications that are not possible to achieve with just classical communication. As an example let us imagine that two persons want to agree on a random bit without anybody else knowing it. If they each possess a qubit from an entangled state $|\phi^+\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$, they get a common random bit by simply measuring their qubit in the same basis. Indeed, once one of the two parties measures its qubit, the state collapses into one of the two states $|00\rangle$ or $|11\rangle$ with equal probability. Hence, while the outcome is random and cannot be known prior to the measurement, they always get the same value. Moreover, the monogamy of entanglement assures the privacy of this outcome. Entanglement creates a sort of private and confidential channel between the parties sharing it.

A crucial goal of quantum network is thus the efficient creation and sharing of EPR pairs. A quantum network may also distribute multipartite entangled states as they are useful for many applications. These states do not only need to be created and shared fast, but the network also has to ensure that they have a sufficient fidelity. Different applications may have different requirements for the fidelity of the states shared by the parties. It may be cheaper for a quantum network architecture to provide EPR pairs whose fidelity is just above the threshold required by a specific application. It is hence the network's responsibility to provide information about the quality of the quantum states that flow through it.

In quantum networks, entanglement is always created locally and then followed by a transfer of one or more of the entangled qubits to the nodes that will process it. In this context, photons are the natural choice for entanglement carriers or so called flying qubits. This is because they are moderately affected by decoherence as well as well supported by current telecom technologies. They can be controlled with standard optical elements and travel at light speed through optical fibers and free-space.

1.3.2 Challenges

One of the main obstacles towards building an international quantum network is long distance communication. The natural way to physically link two nodes in a quantum network is to use optical fibres to carry photons. Unfortunately after a few tens of kilometers, photon loss in fiber becomes predominant and prevents practical applications. The well known PLOB bound [22] gives fundamental limits on quantum communication over long distance in a fiber. The main strategy that is under investigation in the research community is the development of so-called *quantum repeaters*. Formally, we call a quantum repeater a device and a protocol that allows for a better performance than what can be achieved over the direct communication channel alone [23]. In Chapter 4, we will discuss different quantum repeater strategies to link two nodes. We will also study the possibilities of using free space communication, with e.g. satellites or high-altitude balloons in Chapter 6, to overcome the limits imposed by optical fibres.

Photons themselves cannot be stored in an efficient way. Their information must be transferred to a matter qubit and retrieved later. This poses the challenge of creating efficient coupling between light and matter qubits to transfer the data into a long-lived quantum memory. However, since decoherence happens whenever a state is stored in a node of the network, managing the time a qubit has to be stored is also of great importance. In Chapter 4 we will also discuss a possible strategy to limit the storage time of a qubit in quantum network routing. Photons are also subject to noise and loss during their travel. Strategies are under investigation to encode a logical qubit into many physical photons, a process that we usually call *error-correction*. For photonic qubits, some proposals have recently emerged to create a large entangled system whose logical state can be retrieved should some limited amount of loss and noise affect it [24].

Entangled pairs of photonic qubits are the basic unit of networking. Contrary to classical data that can be split into packets on which we can add headers to facilitate the routing, qubits are more difficult to manipulate. This is due to the measurement process and the non-cloning theorem which does not allow to look at what a specific quantum message contains without altering it. Photons thus are hard to route as a photonic light pulse cannot be encapsulated into a packet containing its source and destination as it is done in classical network. In order to route quantum data in a network, specific strategies have to

be designed. They involve precise timing and classical data going along with the quantum data. This will probably give rise to an architecture separated in two planes, a quantum plane in which entanglement will flow and a classical plane to route and control this flow. Routing strategies involving precise timing between classical and quantum data are currently being investigated [25].

Security in quantum networks have to be ensured to some level. It is a critical point because, as we will see in Chapter 2, a lot of envisioned applications for the quantum Internet is improving the privacy of communication. This means that the necessary data to prove security has to be available to the end users. Network protocols themselves should be security aware in order to protect the network itself and limit disruption. In Chapter 3, we will discuss some security properties of a specific network protocol to highlight the difficulty of these considerations.

Quantum devices are far from being widely commercialized and it is likely that they will cost a lot of money and energy during their first phase of development. When designing a quantum network architecture, it is important to keep in mind that end users will probably not have access to fully universal quantum computers. Hence, there is a challenge in designing a network that minimizes the necessary hardware in certain nodes, especially the end user nodes. Moreover, as we saw in Sec 1.1.3, many different physical supports for quantum information are being investigated. It is thus crucial to design standards of communication so that end nodes using different physical systems have efficient interfaces with the network.

Finally, one particular challenge in designing a quantum internet architecture is to make it scalable. This means that there should be a limitation in the number of operations necessary to add a new user to the network. For example if our architecture's topology is a complete graph, meaning that all nodes are connected to each other, adding a new user amounts to create as many channels as there are users of the network. This is unrealistic in a context of thousands of users. Hence, while the ability of entanglement generation between any two nodes should be preserved, some kind of centralized architecture is necessary to make the network scalable. Most of the time the security of network protocols using untrusted nodes, which will necessarily exist in a centralized architecture, is preserved through verification procedures that checks that the nodes are really doing what they are supposed to. We will see examples of this in Chapters 2 and 3.

1.3.3 Advances in quantum networking

These challenges do not prevent important advances in creating quantum networks in local areas. We can for example point out the efforts of the Quantum Internet Alliance [26], a collaboration of several laboratories in Netherlands, Paris, Barcelona, Lisbon, Copenhagen, Geneva, Innsbruck and Stuttgart. They divide their work in creating and linking local quantum networks, designing new protocols and studying the best implementations for the end users or the middle nodes, towards the creation of a European quantum Internet. In Chapter 5, we design and simulate such a pan-European network to study its feasibility and explore the protocols that could already be performed. The Quantum Internet Alliance also works towards building a global vision for the future of the Quantum Internet and has made an attempt at creating a layered structure for the quantum Internet in [27] that we show in Fig. 1.5.

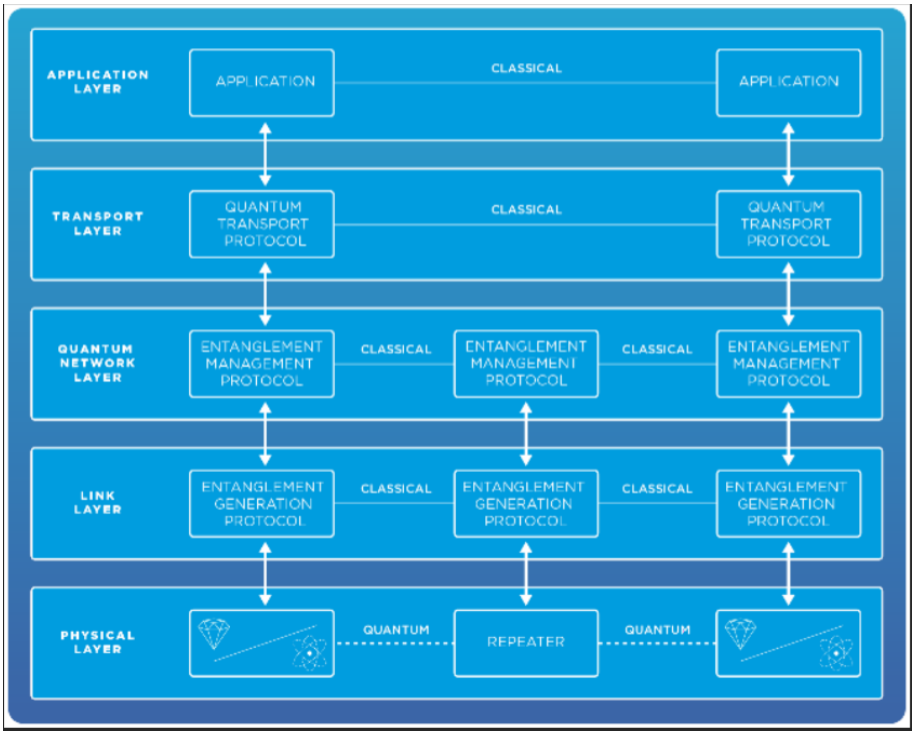


Figure 1.5: A layered model for the quantum Internet from [27]

As the OSI model presented in Fig. 1.3, this layer model helps with the design of a network architecture by imposing standardized interconnection between the different modules. In the final quantum Internet, application designers should not have to be aware of the underlying physical system in which quantum information is processed. Conversely, experimentalists and engineers should not have to care about what the device they construct is going to be used for. With well-defined interfaces, researchers can specialize and focus on optimizing the hardware or protocol running at their own layer.

Theoretical advances include the design of protocols for different layers of this proposed model, for example link layer protocols to establish entanglement between two nodes [28], to route entanglement [25] or to distribute [29] and manipulate [30] multipartite entangled states. The most exciting results are of course in the top-layer, where lies the applications that would impact our daily use of communication networks. In the next chapter we will expand on some protocols achieving functionalities such as Quantum Key Distribution, anonymous transmission or blind and verifiable delegated computation. We however point out here that the ability of performing these protocols depends on the hardware available to the end nodes. It defines stages of development for quantum networks that we show in Fig. 1.6.

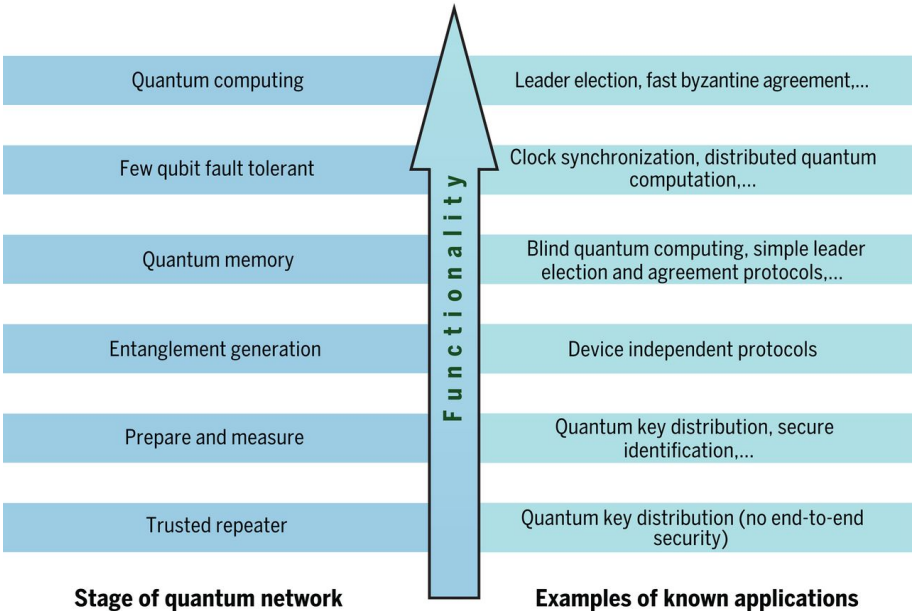


Figure 1.6: Stages of development for quantum network architectures from [27]. Depending on the hardware available of the end nodes (on the left), different protocols can be performed (on the right). As of the date where this thesis is written, we are between the prepare and measure stage and the entanglement generation stage.

As of the date where this thesis is written, quantum computing devices are in the *Noisy Intermediate Scale Quantum* stage (NISQ). This means that we have access to applications using a few tens of physical qubits, with no long-lasting quantum memories. From a quantum network point of view, this corresponds to the ability of sending and measuring photons right when they arrive or to establish entanglement at metropolitan distances. Simulation of such processes are of the essence to understand the precise limits of what we can achieve today and how to push these boundaries. Network simulators such as NetSquid [31] for small quantum networks with precise control on each node, QuISP [32] for large networks and simulation of routing strategies or SimulaQron [33] for software development have emerged to help in this process.

Great advances in designing and simulating complex network protocols are also accompanied by encouraging experimental realisations and progress in photonic hardware [34, 35, 36]. Successful generation of entanglement in metropolitan area have been reported [10, 37] and over 1100km using satellite-based quantum communication [38, 39, 40]. So-called QKD networks allowing the distribution of secret keys are already functioning, for example in Bristol [41] with 8 users, in China[6], or in the South of France. Several projects, focusing on establishing metropolitan quantum networks on a first stage and linking them on a second stage, are in due course. In some time, they should result in the establishment of a global quantum network that we could call quantum Internet.

This thesis is written in the context of quantum Internet development. We try here to contribute to the community by discussing some security concerns and by providing detailed models and simulation studies of quantum internet architectures and protocols. We also try to give a comprehensive introduction to the quantum Internet that encompasses some of its most important aspects. It hopefully highlights important parameters and issues to resolve, while showing what could be realisable as of today.

Chapter 2

Quantum Internet Protocols

In the previous chapter we introduced the quantum Internet, a global network of quantum devices that enhances today's networking capabilities. It brings together a large community of researchers working towards constructing large scale experimental architectures as well as finding new applications for the end users. From information-theoretic secure communication to the delegation of a computation to a distant machine that remains completely ignorant of the computation you're using it for, the quantum Internet's promises are numerous. It should enhance the classical internet by making it more secure and even enlarge the scope of functionalities the users will have access to. Standardized routines to create specific states, integrated chip circuits, protocols to route quantum information through the network or to efficiently verify quantum states, new protocols appear regularly for each layer of the future architecture.

Outline: In this chapter, we go over the details of some quantum internet protocols. We will simulate them in the next chapters to get an idea of what is realizable with current quantum networking technologies. In Sec. 2.1, we first focus on protocols between two parties and give a particular attention to the most studied application of quantum communication, Quantum Key Distribution. We then look into applications making use of more than two parties entanglement in Sec 2.2. For a more exhaustive list of quantum Internet protocols, we refer the reader to the Quantum Protocol Zoo [42], a community-based wiki for quantum internet protocols.

2.1 Bipartite protocols

In this section, the setting will be the following: two users of the quantum Internet, Alice and Bob, are linked through a quantum channel. They both possess quantum devices such as a source of single-qubit states as well as single-qubit processing and measurement devices. They also have access to usual classical computing power as well as the classical Internet. This implies the existence of a classical authenticated channel between Alice and Bob. Most of the protocols work in communication rounds hence we suppose that the parties share a time reference allowing them to time their operations according to defined timesteps.

In this thesis we mostly focus on photonic quantum communication using free space or optical fibers as a quantum channel. In the following, we hence suppose that quantum information is encoded in some degree of freedom of photons, such as their polarization or their arrival time. Thus the quantum devices that Alice and Bob typically hold are single photon sources, passive optical components such as beam splitters and mirrors, and single photon detectors. Photons are subject to loss and noise in fiber and quantum devices that we will model more precisely in Chapters 5 and 6. In this chapter, we however take into account the fact that all photons sent from a party may not arrive to another.

2.1.1 Quantum Key Distribution

The most ubiquitous quantum network application is Quantum Key Distribution (QKD). It is one of the first and most studied applications in quantum communication that has been discovered, with advanced experimental realisations [3, 6, 43] (see reviews [44, 45, 46, 47]). QKD uses quantum phenomena to achieve better security performance than what is possible with classical network protocols. The main goal of QKD is to have a private secret key shared between two parties. As we saw in Sec. 1.2.2, a private key allows two parties to securely communicate over some distance.

QKD has been so extensively studied that there exist many different ways to achieve it. This is an opportunity for us to point out the difference between what we call a *functionality*, which is the application that users want to achieve, and a *protocol*, which is a concrete algorithm explaining step by step how to achieve the functionality. In the following we expand on several protocols achieving the QKD functionality. Note that a good network architecture should allow to choose between different protocols for the same functionality. The users choice could depend on the speed or the level of security that they want to reach.

2.1.1.1 BB84

The first and most standard way for Alice and Bob to generate a shared secret key is to perform the BB84 protocol [48]. By its simplicity, BB84 was the first protocol to raise attention towards quantum communication. It makes use of the quantum measurement process and the no cloning theorem to create a shared private key. It has been extensively used to the point where it has become common to use it as a benchmark for quantum communication channels, as we will do with repeater protocols in Chapter 4. It is also commonly used to teach the advantage of quantum states in communication to young students.

The steps of the BB84 protocol are given below:

BB84

1. At each timestep, Alice chooses a random bit $b \in \{0, 1\}$ and a random base $t \in \{+, \times\}$ and creates qubit $|0\rangle$ if $b = 0$ and $t = +$, $|1\rangle$ if $b = 1$ and $t = +$, $|+\rangle$ if $b = 0$ and $t = \times$ and $|-\rangle$ if $b = 1$ and $t = \times$.
2. Alice sends the state to Bob through an optical fiber
3. At each timestep, Bob randomly chooses a base in $\{\times, +\}$ and perform a measurement on its interface with the quantum channel. Whenever he gets a click, he records the outcome as well as the current timestep and the measurement basis.

After a fixed number of timesteps, Alice and Bob get a so-called *raw key*. They then start performing classical post processing using authenticated classical communication. Bob first sends the list of timestamps associated to each click he got. Alice then discards all the bits that Bob didn't receive and sends the list of basis picked for the remaining bits. Upon receiving this list, Bob sends back the list of basis he used for measuring the qubits he received. They both discard the bits where the basis don't correspond and get the *sifted key*.

Alice and Bob then reveal part of this sifted key to each other. By checking the correlation between these bits, they can check that nobody has peeked into their quantum communication. They abort if necessary, otherwise they construct a private key by performing some rounds of *privacy amplification*.

Privacy amplification is a classical procedure that is used by all QKD protocols to ensure the security of the final key. It is the process of distilling a highly secret key from a partially secure string by public discussion. It consists in applying some common hash function on the remaining bits, which transforms them into a shorter, more secure key. Many privacy amplification procedures are possible [49, 50] but we will not dive into the details of how this is done in this thesis.

2.1.1.2 Entanglement-based QKD

Entanglement-based QKD or Ekert's protocol [51] or BBM92 [52] is a version of QKD where the parties take advantage of entanglement between two qubits. It supposes the existence of a third party, Charlie, who can also simply be seen as source of entangled states. Charlie entangles Alice and Bob by sending them EPR pairs in the $|\psi^-\rangle$ state, one qubit per party. Alice and Bob then measure the arriving qubits in a random basis to get a shared secret key. The main difficulty comes from the fact that both photons from the pair should arrive at their destination. It goes as follow:

BBM92

1. At each timestep, Charlie prepares an EPR Pair in the $|\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$ state.
2. Charlie sends one qubit of the pair to Alice and the other to Bob.
3. Both Alice and Bob receive and measure each qubit randomly in the $\{+, \times\}$ basis. If they get a result, they record the output and the current timestep.

After performing this protocol for some predefined time, Alice and Bob start the classical post-processing. This assumes again the existence of authenticated classical channels. They first announce the timesteps where they got measurement outputs and keep the bits coming from the same pair, which creates the raw key.

Then they publicly announce the basis that they used to measure the states. The rotational invariance of the $|\psi^-\rangle$ state means that Alice and Bob will observe perfect anti-correlation of their outcomes in both bases. By checking that this is the case for a part of the raw key, they can check whether Charlie indeed sent them the expected EPR pairs. Alice and Bob thus keep the rest of the outputs that they measured in the same basis. Finally they can do a round of classical privacy amplification to get the final secret key.

Generation of photonic Bell states is now a rich area of research with very promising performances that make the entanglement-based QKD protocol a good candidate for future key generation. Alice and Bob don't need to trust Charlie in this protocol which is important for guaranteeing the security of the network. However there exists attacks on the detection systems that might affect the security of this protocol. Moreover single-photon detection technologies typically include cryostats that might be demanding for end users. This leads us to the next protocol, where the detection station is moved to the middle node.

2.1.1.3 Measurement-Device Independent QKD

Measurement-Device Independent QKD (MDI-QKD) [53] is a protocol allowing Alice and Bob to create a secret key by sending states to a third party, Charlie, while not trusting him. It relies on Charlie being able to perform Bell-State measurements which are inherently probabilistic in the photonic case. This usually causes the key generation rate to drop. Moreover, without quantum memories the two photons coming from Alice and Bob must arrive at the same time which also lowers the success probability of a MQI-QKD round. Below we write a high-level description of the different quantum operations in a MDI-QKD protocol :

MDI-QKD

1. At each timestep, Alice and Bob both randomly chose a random bit $b \in \{0, 1\}$ and a random base $t \in \{+, \times\}$ and create qubit $|0\rangle$ if $b = 0$ and $t = +$, $|1\rangle$ if $b = 1$ and $t = +$, $|+\rangle$ if $b = 0$ and $t = \times$ and $|-\rangle$ if $b = 1$ and $t = \times$.
2. They both send their state to Charlie so that they arrive at the same time
3. When the qubits arrives simultaneously, Charlie performs a Bell state measurement and communicates the outcome to both parties.

This protocol, together with Twin-Field (TF) QKD, which is conceptually close but relies on single-photon instead of two-photon interference, have received tremendous attention in the recent years as they allow for high key rates over record long distances, even beating the repeaterless bound for the TF case [54, 55, 56]. They are also naturally suited to the progressive vision of quantum networks that can be upgraded as more advanced technology becomes available.

2.1.1.4 Other QKD protocols

The list of QKD protocols does not stop with the three protocols mentioned above. Without going too deep in the details, we would like to mention two more QKD protocols that are commonly used in the lab because they have interesting experimental properties. They both tackle the following issue: it is actually quite difficult to create true single photons states at a high rate.

In practice, laser pulses used in optics generate a stream of light with a number of photons that is probabilistic. Multi-photon emission must be avoided at all cost in QKD protocols because an eavesdropper could then break the security of the key by using so called photon number splitting attacks [57, 58]. Coherent states are statistical superposition of all the possible number of photons in a light pulse. They are used to model photonic states that are coming out of lasers in practice. Weak coherent states are coherent states where the probability of the laser emitting one photon is very small and the probability of emitting more than one photon close to zero. Weak coherent laser pulses are a practical and efficient solution to probabilistically generate a stream of single photons. Following this thought, practical version of BB84 or MDI-QKD *using weak coherent states* have flourished and are now performed in many laboratories.

The probability of emitting more than one photon being small but non zero, the decoy state technique is typically used to improve security [59]. The idea of the decoy state technique is to send multiple intensity laser pulses, resulting in varying photon number statistics throughout the channel, in addition to the BB84 states. By later announcing the intensity used for each pulse, Alice and Bob can measure the error rate of transmitting these decoy states. Parties can thus detect whether a malicious party is attempting to perform a photon number splitting attack.

Finally, the last flavour of QKD that we will mention here is the *Continuous Variable QKD* (CV-QKD) [60, 61]. Quantum information with continuous variable is a paradigm where information is encoded in phase space, or more precisely in the quadrature of an electro-magnetic field. Using so-called homodyne or heterodyne measurements, one can measure the quadratures of the electric field of an incoming light. These measurements can then be used to create a shared secret key. Without entering the technical details of continuous variable states, we mention this QKD protocol for completeness because it is the one currently yielding the highest key rates at short distance while using standard telecom equipment.

2.1.1.5 Security of QKD

The security of QKD protocols comes from the physical quantum nature of the systems that are used. This means that there is no attack coherent with the laws of physics that can break the security. An eavesdropper that collects information about the key by interacting with the quantum signals between the parties can be detected because he would necessarily alter the signals. Alice and Bob can thus detect the presence of a malicious actor and abort the protocol or reject the key when they think that an eavesdropper is present. In this case we talk about *information-theoretic* security, as opposed to security based on computational assumptions on adversarial power that classical key distribution protocols gives (see Sec 1.2.2).

Information-theoretic security, sometimes called unconditional security, is one of the main advantages of quantum networks over classical networks. It assures that no matter what new technology arises in the future (that respects the laws of physics), data transmission will remain secure. This property is often put forward for critical communication such as governmental or military communications where you do not want to assume anything on the adversary computing capabilities. Information-theoretic security guarantees security even if the adversary has unlimited computing power.

The security proofs of QKD protocols can be quite demanding [46, 62], especially in the case of CV-QKD [47]. Since we cannot perform the protocol for an infinitely long time, it has notably to take into account finite size effects. We have to decide whether a malicious actor has tampered with the signals based on a finite number of outcomes. Moreover, because quantum devices are not perfect, we cannot reject a key based on a single incorrect outcome bit. We must still be able to prove that the adversary possesses less information on the transmitted bits than the legitimate parties. There are noise thresholds above which quantum devices don't allow to prove the security of a QKD setup. These proofs are the subject of many research papers and are now quite robust.

There is however one downside to the security of QKD. All QKD protocols are based on the assumption that there exists a classical authenticated channel between the two parties. Authentication itself however relies on a shared secret key, that has to be created using classical protocols. QKD can be used to expand this key into a bigger, useful key. This defeats the purpose of solely relying on physical assumptions that is the main security advantage of QKD. It is also the reason why national cybersecurity agencies such as the French ANSSI [63] reject the standardization of QKD for high-security communications of strategic interests.

2.1.2 Quantum Teleportation

One very important protocol in quantum communication is quantum teleportation [64]. In fact it is so important that it can be considered as a building block of quantum networks. The teleportation functionality transfers information over some distance by consuming a Bell pair. The name of the protocol is a bit misleading as there is no actual teleportation of the information: the protocol still necessitates some classical communication flow to work. It goes as follow:

Quantum Teleportation

1. Alice holds a qubit in the state $|\psi\rangle$. A Bell state is shared between Alice and Bob. Any of the four Bell states $|\phi^+\rangle$,$|\phi^-\rangle$,$|\psi^+\rangle$ or $|\psi^-\rangle$ works.
2. Alice performs a Bell state measurement on the joint state composed of the qubit $|\psi\rangle$ and her qubit from the Bell Pair. She sends the outcome to Bob through a classical channel.
3. Depending on the outcome he receives, Bob performs a correction operation (a X, Z or iY gate) on his qubit from the initial Bell pair.

At the end of the protocol, Bob holds the state $|\psi\rangle$ that Alice had in the beginning, without any quantum communication happening. In fact, due to the entanglement between the qubits of the Bell pair, the Bell state measurement that Alice performs on her two qubits projects Bob's qubit into either $|\psi\rangle$ or a state that is a bit-flip or a phase flip away from the $|\psi\rangle$ state. Knowing Alice's outcome, he can perform the adequate operation to retrieve exactly the state that Alice had initially.

The existence of this protocol has tremendous implications for quantum networking. One might think that the goal of quantum communication through networks is the ability to physically transfer any quantum state from one point to another. Thanks to the teleportation protocol, creating a Bell pair between any two points of the network becomes the main focus. Once a Bell pair is shared between two parties, they can perform this protocol to transfer any quantum state. It simplifies greatly the network architecture. The main goal of a quantum network is the ability to generate entangled pairs between any two nodes of the network.

2.1.3 Enhancing bipartite functionalities

Using quantum properties of photons and particles, the quantum Internet will improve some existing classical functionalities. One of them that has many implications in cryptography and communication is *coin flipping* [65]. It is a fundamental primitive in many cryptography protocols. The goal of coin flipping is to share a uniformly random bit between two parties. It comes in two flavours: strong coin flipping were the parties wish to share a random bit without caring about the actual outcome, and weak coin flipping were each party has a preference for the value of the bit.

In the asynchronous model where we don't assume that players send messages to each other simultaneously but rather in communication rounds, there is no existing classical protocol with cheating probability lower than 1 unless computational assumptions are considered. This means that there is always a way for a dishonest player to force the outcome to be what he wants. In the quantum case where the two parties are linked through a quantum channel, perfect coin flipping is still impossible [66]. However there exist quantum protocols that achieve a cheating probability lower than 1 with already existing experimental realisations [67, 68, 69].

The existence of protocols achieving the coin flipping functionality showcases the ability of the quantum Internet to enhance classical functionalities. It is also the case for other protocols that were widely believed impossible such as *oblivious transfer* [70] and as a consequence *bit commitment*.

In oblivious transfer, the sender sends two bits to the receiver that can choose to receive only one of them. It is said to be secure when none of the two parties gains information that they are not supposed to obtain: the sender cannot know which of his bits has been chosen and the receiver cannot know the value of the bit he has not chosen. Quantum versions of oblivious transfer have been developed [71, 72]. Unfortunately both classical and quantum versions seems secure only within computational assumption.

Yet, quantum versions of oblivious transfer allow for the design of quantum bit commitment protocols. Bit commitment is a cryptography primitive in which a party commits to the value of one bit that is later revealed to another party. It is considered secure when the sender cannot change the value of the bit after he committed to it (binding) and when the receiver cannot know the value of the bit before the

sender allows him to (hiding). Quantum bit commitment protocols also exist, with some positive results in the synchronous model [73]. However, perfect information theoretic security is not achievable even in the quantum case [66].

Research in how to enhance bipartite classical Internet protocols by taking advantage of the quantum encoding of information is a very active research field. It is driven mostly by concerns in privacy preservation. This is indeed the area where quantum enhancement of classical network protocols is believed to be the most useful. But quantum networks will not only enhance classical networks. There exists some completely new possibilities that do not have a classical counterpart, such as the next protocol.

2.1.4 Delegated computation

One of the most interesting features of the future Quantum Internet is that there exist protocols allowing users to privately delegate their quantum computation to any other quantum server they are connected to [74, 75, 76, 77]. Private secure delegation of a computation is defined here as the combination of two features: *blindness*, in the sense that the server does not have full information about the computation, and *verifiability*, in the sense that the user is able to check that the server is performing the right computation. Recent research exhibits promising results towards protocols providing blind and verifiable delegated computation [78], even considering classical clients [79] and security concerns [80, 81]. This would mean that not only the quantum server performing the computation is unaware of what it is actually computing, but also, crucially, the user can check whether the server is doing its task correctly.

In the protocols mentioned above, delegated quantum computation assumes the existence of a powerful server, which usually works in the measurement-based quantum computation paradigm (MBQC) [82]. In this framework, a computation is defined by a series of adaptive measurements performed on universal graph-states. Typically, this server privately receives quantum states from a client that it uses as input to perform some measurement routine involving back and forth classical communication between server and client. By only connecting this new server node to a quantum network through a fiber, any user of the network can securely delegate its computation using a delegation protocol. We recall here the universal blind delegated protocol from [74] allowing a party to blindly delegate its computation to a server node:

Blind delegated computation

1. The user prepares single qubits chosen randomly from $\{1/\sqrt{2}(|0\rangle+e^{i\theta}|1\rangle)|\theta = 0, \pi/4, 2\pi/4, ..., 7\pi/4\}$ and sends them right away to the server.
2. The server receives and entangles the qubits in a predefined universal graph state (e.g. the brickwork state from [74]).
3. Then, for each qubit, the user sends a classical message to the server to tell him in which basis it should measure the qubit. It performs the measurement and communicates the outcome; the user's choice of angles in future rounds will depend on these values. This interaction continues until all the qubits are measured.

The last outcome of the measurements made by the server then contains the result of the classical function the user is computing. If the user is computing a quantum function, the outcome is the last qubits at the server node that he can send back to the user. Provided that the server is able to keep qubits in its memory for a sufficient time, the user only has to manipulate one photon at a time.

The existence of such delegated computation protocols is very exciting because it theoretically allows any user of a network to use a quantum device much more powerful than what he would have access to alone. It permits the centralization of complicated quantum devices in central points of the network, leaving the users with cheaper equipment. This could potentially lead to reducing energy cost of deploying quantum network architectures, by reducing the end user hardware and focusing on efficient delegation of computation.

2.2 Multiparty protocols

Some of quantum network's most groundbreaking applications are multiparty functionalities based on Multipartite Entanglement [4, 83] shared among n parties. Multipartite entanglement comes in many flavours and, just as bipartite entanglement, it produces measurement outputs that have correlations that cannot be predicted with classical theory. These correlations can be used for example to generate a secret key between many parties.

In this thesis we focus on protocols based on the GHZ state given by $\frac{|0\rangle^{\bigotimes n}+|1\rangle^{\bigotimes n}}{\sqrt{2}}$ [5]. It has the particularity that if we trace out one of the qubits from the state, we get a mixed unentangled state which is desirable from a network security point of view. The GHZ state is an entangled state of 3 or more qubits that is used in many protocols where it has been proven to outperform protocols based on bipartite entanglement [84].

Any GHZ-based protocol relies on the ability for a source node to create these states and to transmit them to the users of the network. As many of the multiparty protocols rely on sharing many multipartite entangled states sequentially, the rate of creating and sharing these states is a crucial parameter. Unfortunately, as we will detail a bit more in Chapter 5, GHZ state creation is still at an early stage of research and the rate and fidelity at which these states are created is still too small for practical use. It remains however interesting to investigate how multipartite entanglement can be used to perform new functionalities or how it outperforms some multiparty protocols based on bipartite entanglement.

In this section, we expand on a few GHZ-based protocols. The setting is as follows: n users of the quantum Internet are connected through some architecture allowing the distribution of n-qubit GHZ states at some rate. Each user gets a qubit from the GHZ state.

2.2.1 GHZ state verification

Network protocols making use of the GHZ states usually have two phases: one where a n-qubit GHZ state is shared to n parties, each holding one qubit, and one where local operations and measurements are done by the parties to extract correlated outputs or to transform it to another state. The users can choose to trust that their source is indeed giving them GHZ states or they can incorporate

within their protocol entanglement verification rounds [85]. The latter relies on *verification protocols*, that ensure that the source is indeed creating close to GHZ states. We note that these verification protocols consume many states in order to perform the verification task with sufficient confidence. Hence we see that there is a trade-off between security and rate of performing multiparty protocols. To prevent malicious activity, it is nonetheless crucial to be sure that the state shared is actually a GHZ state.

To be secure, some protocols are based on the technique of performing protocol rounds randomly in between GHZ verification rounds. A malicious party hence is not able to know whether the state he holds will be used for verification or for performing the protocol. The more verification rounds there is, the more secure the protocol becomes. It is thus crucial to have an efficient verification procedure.

In the following we describe a verification protocol using only classical communication between n parties that receive a single qubit each from a source of multipartite entanglement. This protocol is based on the work from [85] where the authors develop and analyze an n-party verification protocol consisting only of classical communication and local quantum operations once the state is shared. One of the parties, called the *Verifier*, has a central role in the protocol: it sends instructions to all parties and broadcasts the output of the verification. We recall the protocol of [85]:

Multipartite entanglement verification protocol

1. The source creates an n-qubit GHZ state and sends each qubit i to party i using a state generation resource and n one-way quantum channels.
2. The Verifier selects for each $i \in [n]$ a random input $x_i \in \{0, 1\}$ such that $\sum_{i=1}^{n} x_i \equiv 0 \pmod 2$ and sends it to the corresponding party via an authenticated classical channel resource. The Verifier keeps one to themselves.
3. If $x_i = 0$, party i performs a Hadamard operation on their qubit. If $x_i = 1$, party i performs a $\sqrt{X}$ operation.
4. Each party i measures their qubit in the $\{|0\rangle, |1\rangle\}$ basis and sends their outcome y_i to the Verifier via the classical channel.
5. The Verifier accepts and outputs $b_{out} = 0$ if and only if

$$\sum_{i=1}^{n} y_i \equiv \frac{1}{2} \sum_{i=1}^{n} x_i (\text{mod } 2)$$

This protocol has been extensively studied and presents desirable properties that are expected from such a protocol: it is correct and for one round, its output depends on the distance between the state that was actually shared by the source and the GHZ state and the number of malicious parties. Precisely, for a state ρ shared among the parties, b_{out} is such that:

$$b_{out} = \begin{cases} 0 & \text{with probability } 1 - \frac{\tau^2}{2} \\ 1 & \text{with probability } \frac{\tau^2}{2} \end{cases} \tag{2.1}$$

with

$$\tau = \min_{U} \text{TD}(|GHZ\rangle\langle GHZ|, U\rho U^\dagger) \tag{2.2}$$

where TD is the trace distance and U is an operator acting only on the space of the dishonest parties.

This protocol is made to be repeated several rounds until some confidence is built on the fact that the source shares GHZ states. In order to prevent the source from sending a wrong state on the round where it is supposed to be used for computation, the authors of [85] considered randomizing this round. They also randomize which party should play the role of the Verifier at each verification round to prevent malicious actions from the parties. Thus, all parties have access to a trusted common random source that gives, at each round, a random bit $C \in \{0, 1\}$ used as a security parameter and an identifier for one party $i \in [n]$. If $C = 0$ (which happens with some probability P_C), the state is used for computation. If $C = 1$ (which happens with probability $1 - P_C$), the parties perform the above verification protocol with i as the Verifier and restart only if the state is accepted. It has been proven that the probability that the protocol has not aborted and that a state ρ such that $\mathrm{TD}(|GHZ\rangle\langle GHZ|, U\rho U^\dagger) \geq \epsilon$ where U is an operator on the space of the k dishonest parties is used for computation is less than $P_C = \frac{4n}{k\epsilon^2}$.

The security properties in [85] are proven in a game-based framework hence are not composable as we will expand more in Chapter 3. There is for example a strategy where, when performing the protocol multiple times in a row, a malicious coalition of parties and source could increase the probability that the honest parties accept a state that is not a GHZ state. It has indeed been noticed that if we allow for a 50% loss rate in the quantum communication, there exists a strategy for dishonest players that increases their probability of making the others accept a faulty state. This problem has been later solved in [86] where a loss-tolerant variation of this protocol that presents the same security properties, called the θ-protocol, was implemented in a photonic setting. It mainly consists in changing the classical instructions $X = \{x_i\}_{i=1}^n$ sent by the Verifier to angles $\Theta = \{\theta_i\}_{i=1}^n$ indicating the rotated measurement basis for each party. This protocol increases the loss that can be tolerated by the protocol, but still the dishonest parties can increase their cheating probability if the losses are high enough.

2.2.2 Conference key agreement

The Conference Key Agreement (CKA) functionality is the multipartite counterpart of Quantum Key Distribution. It allows n parties to get a shared secret key that they can use for secretly communicating or any other application. CKA can be achieved by a composition of bipartite QKD protocols but it is proven that using multipartite quantum correlations can lead to more efficient protocols [84]. There exists a variety of protocols achieving this functionality (see [87] for an extended review) including GHZ-based protocol [88, 89] with an experimental realization [90].

The main ingredient to get a conference secret key in these protocols is GHZ state sharing and measurement. Indeed, a n-qubit GHZ state is given by the superposition of all the qubits in the state $|0\rangle$ and all the qubits in the state $|1\rangle$ (see Eq. 1.6). This means that prior to the measurement of one of the qubits, any qubit measurement outcome is random. However once one qubit has been measured, all the other qubit measurements will give the same output. Hence if a GHZ state is shared to n parties, they all get a private common random bit when measuring their qubit.

By repeating this process multiple times, the n users can get a raw key. Just as in QKD protocols, the n parties can then extract a common secret key by performing classical rounds of communication and privacy amplification protocols. This key can be used for multiple purposes such as private communications

or as a block of a more complex protocol (e.g. a common random number generator). As it consists in sharing and measuring GHZ states, the rate of a CKA protocol can also be used as a benchmark for a network architecture with many parties.

2.2.3 Anonymous transmission

This anonymous transmission functionality allows two users of the network, a sender and a receiver, to establish a link that they can use for transmitting anonymously a message qubit via teleportation [91, 92]. Here we present a GHZ-based protocol achieving anonymous transmission from [93]. The quantum message is transmitted in a way that the identity of the sender is unknown to every other node, and the identity of the receiver is known only to the sender. It relies on classical pre-processing allowing the sender to notify anonymously the receiver that he is going to receive something. Here we don't describe nor simulate this classical pre-processing and we refer the reader to [93] for more information.

Anonymous Entanglement

1. A source creates and shares an n-qubit GHZ state.
2. Every user except the sender and the receiver applies a Hadamard gate to their qubit. They measure it and get outcomes m_i that they broadcast.
3. The sender picks a random bit b and broadcasts it. She applies a Z gate to her qubit if $b = 1$.
4. The receiver picks a random bit b' and broadcasts it. He applies a Z gate to his qubit if $b \oplus \bigoplus_i m_i = 1$

After performing this protocol, the sender and the receiver anonymously share a Bell pair that they can use to teleport any other state. This relies on the fact that they are able to keep their qubit for the time of the protocol. If on-demand quantum storage is not available at the user nodes, for example in the photonic architecture that we present in Chapter 5, non-optimized solutions like delay lines can be used for this task.

Repeating the Anonymous entanglement protocol enough times in between GHZ verification rounds allows for provably secure anonymous transmission of quantum information. However, the number of GHZ states necessary scales badly with the number of parties and the size of the message to transmit. This is because the verification protocol presented above is costly in GHZ resources. We will however see in Chapter 5 that it is still possible to perform a few rounds of this protocol in less than an hour with 4 parties and today's hardware capabilities. Recently, some work has been done to replace this expensive verification phase with BB84 based test [84] which might bring more attention towards the protocol presented in this section.

2.2.4 Other multipartite protocol

We are still at the dawn of research in quantum networks and we are still not fully aware of what they will allow us to do. A lot of theoretical work is currently achieved to study how to distribute [29] and manipulate [30] multipartite entangled states. New applications extracted from many-particles entangled state manipulation and measurement appear frequently in the literature. We cite some of them in this section for completeness while not pretending to be exhaustive. We don't go over the precise

details of these protocols as we will not simulate them in the next chapters and some of them are still technologically out of reach.

One interesting enhancement that quantum networks get over classical multipartite capabilities is the existence of quantum *Byzantine agreement* protocols. Byzantine agreement [94] is a cryptography problem where n parties at some distance have to agree on a value given by one of them even when some parties are malicious. Deriving from the image of a general having to pass a message to some possibly malevolent lieutenants, the byzantine agreement is a fundamental primitive in cryptography and distributed computing. Several protocols making use of the special properties of quantum information exist and show performances exceeding classical network protocols. For example, there exists a fast quantum byzantine agreement [95] with a constant number of communication rounds, where classical algorithms have a scaling in $\Omega(\sqrt{n}\log n)$. There also exists an elegant 3-party solution using entangled qutrits [96] as well as solutions based on bipartite entanglement [97], CV-based solutions [98] and basic experimental realisations [99].

The existence of weak coin flipping protocols allow the design of leader election protocols [100] which would allow a secure random selection of a party in a network. In the same spirit, a secure electronic voting GHZ-based protocol has been proposed recently [101]. Multiparty delegated classical [102] and quantum [103] computation protocols using quantum resources have also been proposed. These services are often pointed out as distrustful in classical networks. The fact that we can design secure quantum alternatives could have some impact on our daily lives.

Some applications are still in development and we cannot infer the impact that they could have on our daily lives. An example of such protocol is the investigation and experimental realisation of a Quantum Money protocol [104, 105], which would allow unforgeability of quantum banknotes and credit cards. It is also hard to grasp the impact of synchronized clock networks [106, 107, 108, 109] on the efficiency of networking processes. Unfortunately current technological capabilities, especially in creating long lasting quantum memories and efficient GHZ state generation, are not yet up for the task of performing useful realisation of such protocols. This however bears exciting promises for future capabilities.

Chapter 3

Security Considerations

Security is one of the main advantages offered by quantum networks. Quantum processing of information makes security rely on the physical laws of nature instead of relying on computational assumptions. An important security notion that has interested scientists recently is the so-called composable security. It is a strong version of security that allows to take protocols as black boxes that we could use as building blocks to design bigger protocols without having to prove security at a high level. In this chapter, we study the composable security of the multipartite entanglement verification protocol presented in the previous chapter. Composable security of this protocol would be very useful as it is used by many other network protocols to ensure that the honest users indeed share entanglement before proceeding to the actual protocols. Unfortunately we could prove composable security only against a malicious source. The case of dishonest parties possibly colluding with a dishonest source raised questions about the limits and practicality of composable security.

Contribution and outline: Our main contribution in this work is a comprehensive study of the composable security of a multiparty protocol. Most current composable security studies at this time were only bipartite. We also give a pedagogical introduction to the Abstract Cryptography framework, used to prove composable security. We however point out the limitation of our study that was based on an understanding of the Abstract Cryptography framework that has evolved with new discussions and results. We start by motivating the use of the Abstract Cryptography framework of which we give a complete introduction in Sec. 3.1. We then move on to prove the composable security of the multipartite entanglement verification protocol when we consider the source to be possibly malicious in Sec. 3.2. We also construct a resource giving verified GHZ states to the parties accessing it, which is more practical for using in bigger protocols. Finally, in Sec. 3.3 we discuss the realism of our result, the case of more malicious parties and the evolution in our understanding of the notion of composable security.

Article link : The full article can be found at https://arxiv.org/abs/2004.07679 and is published in Physical Review A. (Phys. Rev. A 103, 052609, May 2021)

3.1 Abstract Cryptography Definitions

To prove the composable security of a protocol, the usual setting used in cryptography does not suffice. We need to shift to new paradigms in which composable security comes within the security proof. In this section we give an introduction to the Abstract Cryptography framework, one such composable framework.

3.1.1 The usual game-based setting Vs composable security

In communication and cryptography, security of a protocol is usually defined as the ability to resist certain attacks. By carefully designing relevant scenarios and adversary capabilities, one can then compute the amount of information it has access to. Using game theory, it is possible to prove that the maximum information a malicious party could have about the secret data of a protocol is not enough to break the security. When we do so, we prove security in a *game-based* framework. This proves security against a certain family of attacks.

While being quite strong already and sufficient for most practical uses, security properties proven in a game-based framework leave the door open to attacks exploiting for example the repetition of a protocol multiple times. This is where composable security comes into play. A protocol is said to be *composably secure* if it can be repeated multiple times in a row or if it can be used as a subroutine of a bigger protocol without threatening the overall security. The protocol is thus seen as a black box with definite inputs and outputs. This box can be put in series with other composably secure boxes. This amounts to performing protocols one after the other.

In order to prove composable security, one needs to prove security in a composable framework. One such framework is Abstract (or Constructive) Cryptography (AC), a top-down approach developed by U. Maurer and R. Renner [110, 111, 112] to define a so-called simulation-based cryptography theory. It creates some notion of a module with well-defined interfaces that interacts with the rest of the world in a black box fashion. In the Universal Composability framework of Canetti [113], another composable framework, this is called a functionality. In AC, those modules are called resources and going from a resource to another is done through converters called protocols. For example a one-time pad protocol constructs a secure communication channel resource out of a secret key resource and an authenticated classical channel (see Fig. 3.1). In their first paper [110], Renner and Maurer defined a complete cryptography algebra of resources with their composition rules. This allowed them to define *equivalence relations* between resources and to infer security notions that inherit composability properties. Moreover this framework is of interest when modeling multiparty protocols as it offers a simpler view of what dishonest parties could have access to than the usual game-based cryptography theory where the strategy for a dishonest group should be given explicitly. The level of abstraction of the different resources can be modulated to highlight the properties that one wants to study about them. Finally, the AC framework is a resource theory with a large power of abstraction that allows us to think of a protocol the same way we would do when thinking of an application in the quantum Internet.

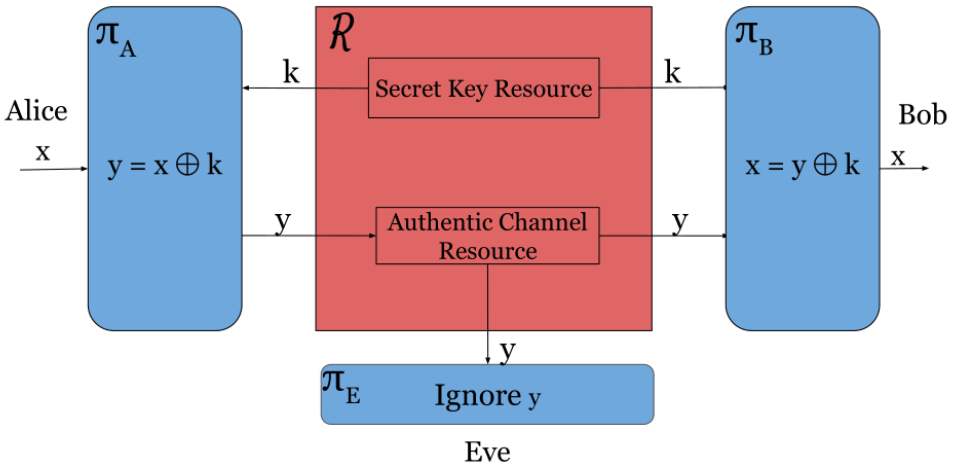


Figure 3.1: Concrete One Time Pad resource $\pi_A\pi_B\mathcal{R}\pi_E$: Alice has access to the left interface, Bob to the right interface and Eve to the down interface. $\mathcal{R}$ is the resource composed of a secret key resource and an authentic channel resource in parallel. Protocols are represented in blue, π_E being the protocol of an honest Eve that blocks the input y from the authenticated channel resource.

Different results have been achieved using this framework such as the study of unfair coin tossing [114], remote state preparation [115], oblivious transfer [72] and composable security of multiparty delegated quantum computing [103, 81, 116]. Different extensions have also been proposed such as adding relativistic constraints [117] or global event history in the case of ratcheting [118]. Let us give a brief overview of this framework which we will use to study our multipartite entanglement verification protocol.

3.1.2 The Abstract Cryptography framework

Abstract cryptography uses the concept of abstract systems to express cryptography as a resource theory. A cryptography protocol is viewed as the construction of some *ideal* resource $\mathcal{S}$ out of other *real* resources $\mathcal{R}$. This construction notion is made through converters. Finally, the distance between two resources is formalised through the notion of a distinguisher. Those three objects are the building blocks of the AC theory.

A **resource** is an abstract system with interfaces specified by a set $\mathcal{I}$ (e.g. $\mathcal{I} = \{A, B, E\}$ for Alice, Bob and Eve in a tripartite setting). Each interface is accessible to one user and provides them with some abilities. Note that the notion of a party is not explicitly modeled in this framework, but induced by the interfaces they are restricted to have access to. Resources are used to model functionalities that are not done specifically by a party. They can be associated with real physical resources (e.g. a quantum channel) or with abstract functionalities (e.g. bit commitment or quantum random number generation). The level of abstraction of such a functionality is not bounded *per se* but it is usually tailored to the application that one is modeling and the properties one wants to highlight. For example quantum memories can be explicit and represented with resources or abstracted in converters. Classical protocols can also be explicitly shown or abstracted through oracle calls. Moreover any parallel composition of resources is a resource in which the interface set corresponds to the union of the ones from the composed resources. A resource is said to be concrete if it is a composition of other resources representing an actual protocol

performed in the real world. Otherwise, if it is simply a box representing a functionality, we call it ideal. Most of AC thus consists in studying how close a concrete resource is to an ideal resource.

Converters are also abstract systems with one set of "inside" interfaces that are expected to be connected to a resource and one set of "outside" interfaces. Their name derives from the fact that a converter attached to a resource converts it into another resource by emulating a certain set of interfaces to the outside world. Attached on a concrete resource, they typically model the local computation of a party during a protocol and are denoted with Greek letters. For a resource $\mathcal{R}$ with interfaces A and B and a two-party protocol $\pi = \{\pi_A, \pi_B\}$ we denote $\pi_A \mathcal{R} \pi_B$ the resource obtained from connecting π_A to interface A and π_B to interface B (see Fig. 3.1). A dishonest party is then modeled by just unplugging their corresponding converter from the resources, indicating that the party is not following the protocol. This leaves the interface they have been accessing open to the outside world. Note that the ordering of the converters is not important and that they are usually written in the most readable way.

Converters are also used to model the honest utilisation of an ideal resource. Indeed, a dishonest party is modeled by unplugging its converter from the concrete resource, opening new interfaces. To model this on the ideal resource associated we use a converter, called a *filter*. Filters cover some interfaces of an ideal resource for an honest player, and are removed in the case of a dishonest utilisation of the resource (see an example in Fig. 3.2). Finally, converters are used in the ideal world as a tool in the proofs to simulate the local output to a dishonest party. In this case we use the term of *simulator*. Converters and resources can be described with the help of boxes and arrows as well as in the form of algorithms by specifying where each output goes.

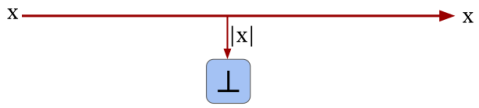


Figure 3.2: Filtered one-way private classical channel resource. It is an ideal resource taking as input a bitstring x at the left interface, outputting it at the right interface and leaking its size $|x|$ on the bottom interface. $\perp$ is a filter blocking the bottom interface to simulate an honest use of the resource. In the case of a dishonest use of this resource, i.e. an eavesdropper trying to get x, $\perp$ is removed and $|x|$ becomes accessible. This models all the information this eavesdropper can get out of this resource. As we will see in the next section, this resource is equivalent to the one of Fig. 3.1.

Abstract cryptography is the theory of breaking down cryptographic processes into box-shaped resources that can be composed together in series or in parallel. Resources, which represent cryptographic primitives, can be transformed into other resources using converters and usual algebraic composition rules. A *concrete* resource represents an actual protocol using physical systems and classical and/or quantum operations while an *ideal* resource is the abstraction of the functionality achieved by the protocol. We say that a protocol $\pi = \{\pi_A, \pi_B\}$ constructs the resource $\mathcal{S}$ out of $\mathcal{R}$ and write $\mathcal{R} \xrightarrow{\pi} \mathcal{S}$. Such a construction is *composable* if for all $\mathcal{R}, \mathcal{S}$ and $\mathcal{T}$ resources and π, ν converters (protocols) such that $\mathcal{R} \xrightarrow{\pi} \mathcal{S}$ and $\mathcal{S} \xrightarrow{\nu} \mathcal{T}$ we have that

$$\mathcal{R} \xrightarrow{\pi} \mathcal{S} \wedge \mathcal{S} \xrightarrow{\nu} \mathcal{T} \implies \mathcal{R} \xrightarrow{\nu \circ \pi} \mathcal{T}. \tag{3.1}$$

3.1.3 Security definition and assumptions

To show that a protocol π constructs the ideal $\mathcal{S}$ out of concrete resource $\mathcal{R}$, we have to capture an equivalence notion, with a metric $\approx$ such that $\pi\mathcal{R} \approx \mathcal{S} \overset{def}{\iff} \mathcal{R} \xrightarrow{\pi} \mathcal{S}$. To that end, Abstract Cryptography introduces its last abstract system: **Dinstiguishers**. They are used to construct a pseudo-metric between two resources. They replace the notion of an adversary and also encompass any protocol that is run before, after or during the protocol being analyzed. As its name indicates, a distinguisher is used to distinguish between two resources $\mathcal{R}$ and $\mathcal{S}$ by connecting to all their interfaces and outputting a single bit: a guess whether it is interacting with $\mathcal{R}$ or $\mathcal{S}$ (see Fig. 3.3). The advantage of a distinguisher $\mathbf{D}$ is given by

$$d^{\mathbf{D}}(\mathcal{R}, \mathcal{S}) = |Pr[\mathbf{D}\mathcal{R} = 0] - Pr[\mathbf{D}\mathcal{S} = 0]|,$$

where $\mathbf{D}\mathcal{R}$ is the output of $\mathbf{D}$ when interacting with $\mathcal{R}$. For example in Fig. 3.3, replacing $\mathcal{R}$ with $\pi_A\pi_B\mathcal{R}\pi_E$ from Fig.3.1 and $\mathcal{S}$ with the filtered private authenticated classical channel resource from Fig. 3.2, we see that any distinguisher $\mathbf{D}$ will see the same output x for any given input x on any of the two resources. Hence we have that $d^{\mathbf{D}}(\mathcal{R}, \mathcal{S}) = 0$. For a class of distinguishers $\mathbb{D}$, the distinguishing advantage is defined as

$$d^{\mathbb{D}}(\mathcal{R}, \mathcal{S}) = \sup_{\mathbf{D} \in \mathbb{D}} d^{\mathbf{D}}(\mathcal{R}, \mathcal{S}).$$

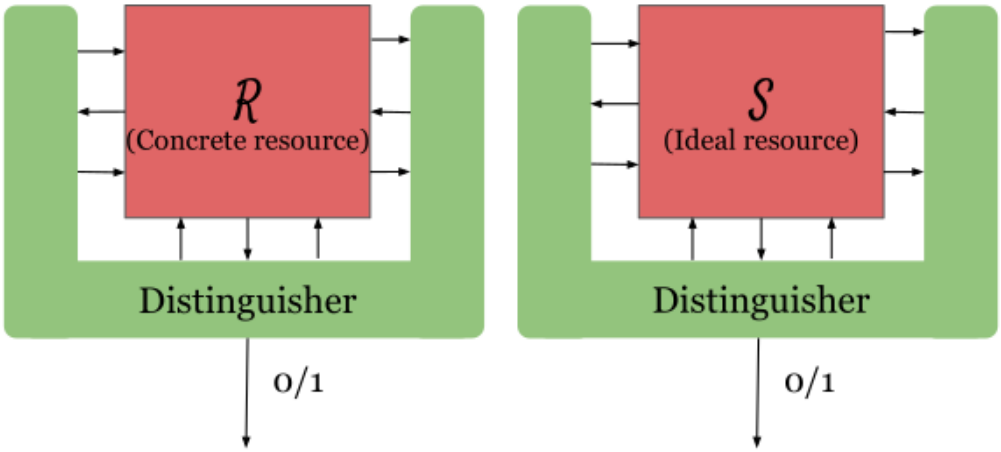


Figure 3.3: A distinguisher interacting with $\mathcal{R}$ and $\mathcal{S}$. It has access to a complete description of the two systems and can choose the inputs of all players, receive their outputs and simultaneously fulfill the role of an adversary. After interaction, it must guess which resource is which. Replacing $\mathcal{R}$ by Fig. 3.1 and $\mathcal{S}$ by Fig. 3.2, no distinguisher is able to guess between the two resources.

The distinguishing advantage is a pseudo-metric on the space satisfying all properties of a composable distance, namely identity, symmetry and triangle inequality. This allows to define *equivalence relations* between resources: for a class of distinguishers $\mathbb{D}$ we say that $\mathcal{R}$ is equivalent (or ϵ-close to) $\mathcal{S}$ and write $\mathcal{R} \approx \mathcal{S}$ (resp. $\mathcal{R} \approx_\epsilon \mathcal{S}$) if $d^{\mathbb{D}}(\mathcal{R}, \mathcal{S}) = 0$ (resp. $d^{\mathbb{D}}(\mathcal{R}, \mathcal{S}) \leq \epsilon$).

To summarize, converters describe mostly local and non-costly operations while resources can have non local functionalities and extended computational power. Distinguishers are all powerful objects that represent the environment trying to guess between two resources.

We now have the necessary ingredients to present the notion of secure construction of a resource in AC. Let $\pi = \{\pi_i\}_{i=1}^n$ be a protocol run by n parties using the concrete resource $\mathcal{R}$ and let $\mathcal{S}$ be an ideal resource with all the desired properties expected from the protocol. $\mathcal{R}$ and $\mathcal{S}$ have interfaces $\mathcal{I}$. We say that π **securely constructs** $\mathcal{S}$ **out of** $\mathcal{R}$ **within** ϵ and write $\mathcal{R} \xrightarrow{(\pi,\epsilon)} \mathcal{S}$ if there exist converters $\sigma = \{\sigma_i\}$ called *simulators* such that

$$\forall \mathcal{P} \subseteq \mathcal{I}, \pi_{\mathcal{P}} \mathcal{R} \approx_\epsilon \sigma_{\mathcal{I}\setminus\mathcal{P}} \mathcal{S}, \tag{3.2}$$

with $\forall \mathcal{P} \subseteq \mathcal{I}, \pi_{\mathcal{P}} = \{\pi_i\}_{i\in\mathcal{P}}$.

This means that if only a subset $\mathcal{P}$ of parties follow their protocol π_i (left-hand side of Eq. 3.2), we are able to find simulators on the rest of the interfaces $\{\sigma_j\}_{j\in\mathcal{I}\setminus\mathcal{P}}$ such that this equivalence holds (right-hand side of Eq. (2)).

The simulator σ_j locally simulates on the ideal resource the interfaces the party has access to on the concrete resource when party j is dishonest. Simulators don't represent actual concrete operations and should only be seen as a tool in the proof. For example, using a simulator σ taking as input a size and producing a random bit string of this size, we have an equivalence relation between the concrete one-time pad resource with an dishonest Eve $\pi_A \pi_B \mathcal{R}$ and the ideal private classical channel resource on which we attach σ (see Fig. 3.4). This equivalence together with the equivalence of Fig. 3.1 and Fig. 3.2 (usually denoted as the correctness of the protocol) proves the composably secure construction of the private classical channel resource by the one-time pad protocol. In this case, those two equivalences suffice because we suppose Alice and Bob to be always honest in the one-time pad protocol. One must find simulators for each subset of possible dishonest parties to prove composable construction.

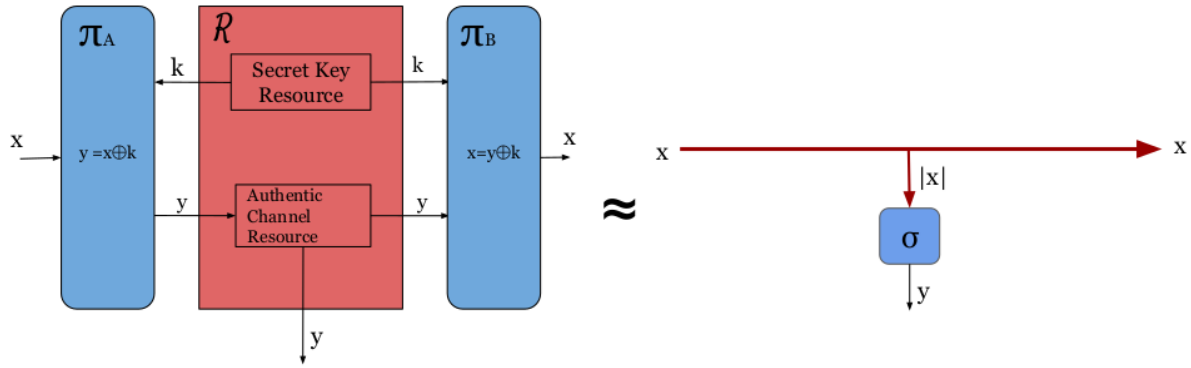


Figure 3.4: Equivalence between the One-time pad resource with a dishonest Eve and the ideal private classical channel resource with the simulator σ.

The power of the class of distinguishers and simulators used to prove a secure construction determines the strength of the security proof. For example considering only classical distinguishers leads to security against classical adversaries while considering all powerful distinguishers leads to information-theoretic security. Ideally we would want the class of simulators to be restricted to a class of easily implementable converters and the set of distinguishers to be as general as possible. This leads to security statements such as "We can easily construct the ideal resource $\mathcal{S}$ from $\mathcal{R}$ and we can easily simulate any cheating behaviour such that even a very powerful distinguisher cannot tell the two resources apart".

3.2 Composable security of Multipartite Entanglement Verification

In this section, we introduce the ideal and concrete resources, and finally prove the secure construction. We recall that the multipartite entanglement verification protocol consists in one party randomly designated as the verifier sending classical signals to all other parties, gathering measurement outputs of the shared state from the other parties and outputing a bit indicating if the shared state was a GHZ state. The protocol is detailed in Sec. 2.2.1. In the following, we will call "Source" the party controlling the entanglement source or the device itself interchangeably. We will consider authenticated classical communication and perfect quantum communication as any imperfection can be modeled as the source perfectly sending noisy states.

We believe the following proof can be adapted to any stabilizer state verification where parties first receive a qubit and then do only local operations and classical communication (LOCC). For simplicity we will consider only the version of the protocol presented in Sec. 2.2.1 (called the XY-protocol) but the following proof can be straightforwardly extended to match the θ-protocol as well.

3.2.1 Ideal Resource

Let us now present the ideal resource for practical multipartite entanglement verification. Consider a source using physical resources to create and share an n-qubit quantum state to n parties expecting a qubit from a GHZ state. Our resource, called $\mathcal{MEV}_C$, aims to get a sense of how trustworthy the source is, by verifying that it sends a state at least close to the GHZ state. It also has a built-in parameter C that makes the resource output qubits with some probability known by all $n+1$ parties using the resource.

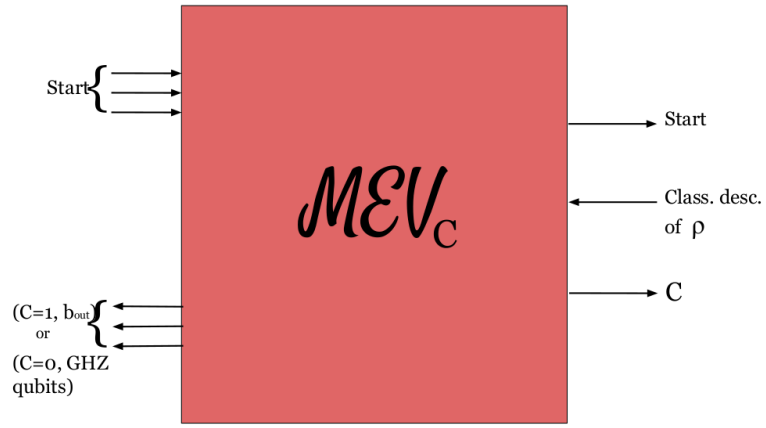


Figure 3.5: The $\mathcal{MEV}_C$ resource for $n = 3$ parties. For readability we put the parties interfaces on the left and the source interface on the right. The left interfaces are "collective interfaces" meaning that inputs are sent collectively by all the parties and the output is obtained by all parties.

This black box (see Fig. 3.5 for a 3-party example) has $n + 1$ input interfaces. All n parties wishing to test a source collectively send a start signal to the input interfaces of resource. The last interface is the source interface that gets a classical description of the state sent by the source. Upon reception of the start inputs, $\mathcal{MEV}_C$ will forward the start signals to the source interface then wait for the classical

description of an n-qubit quantum state ρ. After that, it outputs on all interfaces a bit $C = 0$ with probability p, or $C = 1$ with probability $1 - p$. This bit indicates if the resource is going to output qubits or a verification bit b_{out}. The probability distribution of C can be tuned freely to match any distribution. If $C = 0$ it then outputs to each party a qubit of ρ and if $C = 1$ it computes a bit b_{out} indicating if the state shared by the source is close to the GHZ state and sends it to all parties. This box is made to be composed with itself in series with a very small p until all parties get a qubit or $b_{out} = 1$.

The output bit b_{out} should indicate whether the state shared by the source is ϵ-close to the GHZ state for some ϵ. At this level of abstraction, we don't care whether this behaviour comes from a faulty device or an actual adversary trying to manipulate the source. Our $\mathcal{MEV}_C$ resource outputs a b_{out} such that

$$b_{out} = \begin{cases} 0 & \text{with probability } 1 - \frac{\tau^2}{2} \\ 1 & \text{with probability } \frac{\tau^2}{2} \end{cases} \tag{3.3}$$

with

$$\tau = \mathrm{TD}(|GHZ\rangle\langle GHZ|, \rho), \tag{3.4}$$

where TD is the trace distance. The output of the resource is thus probabilistic, and depends on the trace distance between the input state ρ and the GHZ state and on the security parameter C. Notice that this b_{out} follows the same distribution as the one of the original protocol (see Sec. 2.2.1) in the case where all parties are honest. The security parameter C is added to the verification procedure to make the resource suitable for practical use in larger protocols where one wants to eventually get shared entanglement between the parties when the source is acting correctly.

Now in the case of the honest use of the resource, the source interface is given as input a classical description of the GHZ state. Moreover the output C remains hidden to the outside world. In AC this is modeled by using converters, the so called *filters*, that block the adversarial interfaces (thus filtering the outputs) and send a specific input. In our case we define one filter $\perp$ that enforces the honest use of $\mathcal{MEV}_C$. It blocks any deviation from the outside world and upon reception of a start signal, it sends a classical description of a GHZ state to $\mathcal{MEV}_C$ (see Fig. 3.6). It has its inside interface plugged into the $\mathcal{MEV}_C$ resource and its outside interface open to inputs from any distinguisher (see [118] for extended discussion about filtering and the inclusion of events in AC).

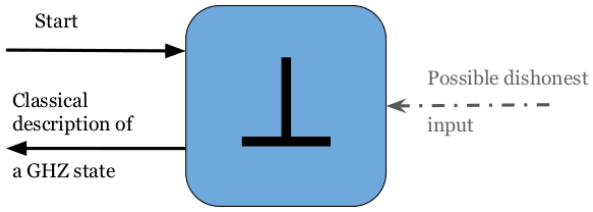


Figure 3.6: Filter $\perp$. Upon reception of a start input, it outputs a classical description of a GHZ state on its inside interface and blocks any input at its outside or inside interface.

Composed with $\mathcal{MEV}_C$, they form our ideal resource $\mathcal{MEV}_C\perp$ for secure verified GHZ sharing or source testing (see Fig. 3.7 for a 3-party example).

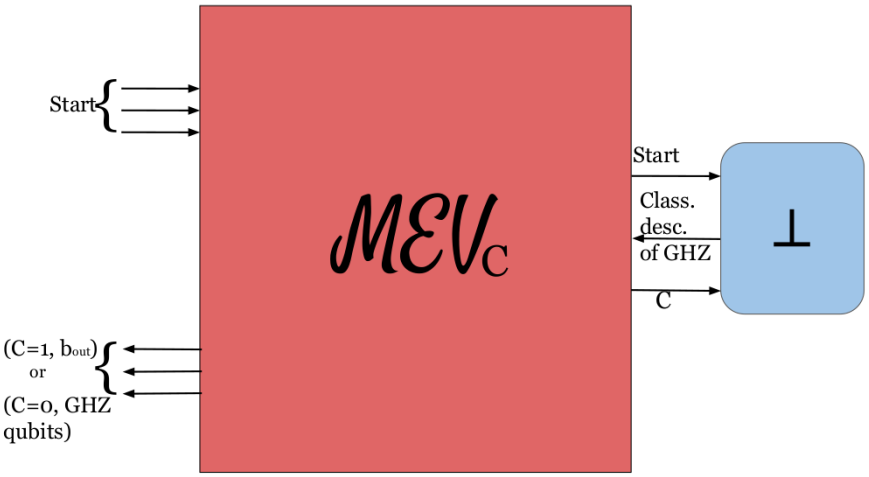


Figure 3.7: The ideal filtered $\mathcal{MEV}_C\perp$ resource for $n = 3$ parties. On the left are the "collective interfaces" that are used by the parties to collectively send the start signal and receive the output. On the right is the source interface filtered by $\perp$, that blocks any input and sends a specific message to the resource.

3.2.2 Concrete Resource

We will now make explicit the protocol in the AC framework, by defining the resources used and the converters for each party. We first define the concrete resources, which in this case are abstractions of physical resources. More explicitly we define the state generator resource, the one-way quantum channel resource, the two-way classical channel resource and two multiparty classical computation oracles.

The state generator ($\mathcal{SG}_n$) resource (see Fig. 3.8) represents a perfect source of quantum states able to create arbitrary quantum states of at most n qubits. Receiving a classical description of an n-qubit state ρ on its input interface it will output each qubit of ρ on its n output interfaces. This resource can be used to model imperfect sources by including the noise in the classical description of the state given as input. We consider that no information is leaked by this resource about the state that it creates, as it is the more restricting scenario in our security proof. In Sec. 3.3.3 we discuss the realization of such a resource.

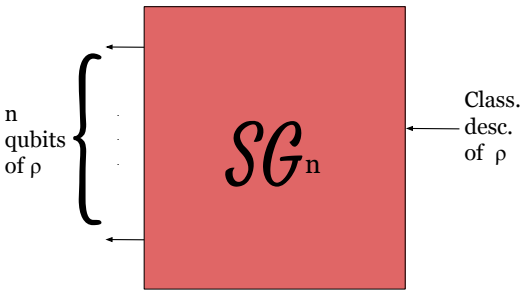


Figure 3.8: State generator resource.

The $\mathcal{SG}_n$ resource is to be composed with n quantum channel resources which we draw as arrows with a Q (see Fig. 3.9). A quantum channel resource in our case is an ideal resource representing a perfect private authenticated quantum channel. It takes as input a qubit and outputs the same qubit at a different place without any leakage. We don't make here any assumption on how these resources are realised. They could be constructed out of quantum repeater protocols or out of a good fiber and an error-correcting protocol depending on the distance between the source and the parties. AC typically allows us to abstract these considerations in the context of this work, though we assume that such an ideal resource can be realised.

Figure 3.9: Quantum channel resource.

Finally the classical communication between parties is modeled through classical channel resources which we simply draw as arrows (see Fig. 3.10). They take bits at any of their interfaces and transmit them to the other interface. We suppose those channels to be authenticated: to any other party watching the channel, it will also output of the message transmitted without the possibility to alter it. In order not to overload the figures, we don't represent this leaking interface when all parties are honest but we do when considering a dishonest source watching over the classical communication.

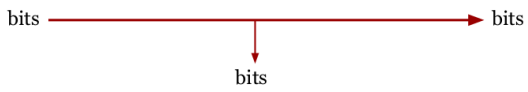


Figure 3.10: Classical channel resource.

We will abstract multiparty classical functionalities achieved by the parties by the use of oracle queries. All parties can collectively call two oracles $\mathcal{O}_C$ and $\mathcal{O}_v$ that respectively give a common random bit C and a common random party identifier v to each party. We will draw them as boxes with n input interfaces expecting a collective query from the parties and n output interface broadcasting C or v. This is a modeling of classical communication protocols that provide random bits and random identifiers to the parties. It is not considered private and the values of C and v are available to any malicious party watching over the classical communication. We will discuss how these oracles can be replaced by actual classical protocols in Sec. 3.3.3. Moreover, each party is locally equipped with a quantum register able to perfectly store a qubit for the time required by the protocol on which they can perform one-qubit operations and measurements. Quantum registers will not be drawn in the figures for simplification purposes as well as the leakage interfaces of the classical channels, but they should not be forgotten as assumptions in our model, particularly when considering the case of a malicious party. Since we consider here all parties to be honest during the verification protocol, we only draw resources and interfaces of interest.

We call $\mathcal{R}$ the resource constructed by a state generator resource composed in series to a collection of n quantum channel resources and in parallel to n classical channel resources, $\mathcal{O}_C$ and $\mathcal{O}_v$. $\mathcal{R}$ formally defines the creation of a state, common classical randomness generator protocols, the (2-way) classical communication between the Verifier and the parties and the (one-way) quantum communication between the source and the parties.

The next step is to present the converters $\pi = \{\pi_i\}_{i=1}^n$ and π_S that represent the protocols followed by each party and the source. They model the local computation of each party during an honest round of the protocol and can be represented either as algorithms or as boxes and arrows, that both expect some input from which they produce output to send to the resources. Their quantum abilities are equal to the ones that we give to local parties performing the multipartite entanglement verification protocol [85].

We start with $\pi = \{\pi_i\}_{i=1}^n$ representing the protocol followed by each party i (See Protocol 2). i is a binary identifier for each party, but for simplicity we represent it with $i \in [n]$ and we write $\pi_{[n]}$ for the parallel composition of all $\{\pi_i\}_{i=1}^n$.

Protocol for the i_{th} party π_i

1. Ask the source to send a GHZ state. Wait for the reception of the qubit.
2. After reception, query $\mathcal{O}_C$, get C and output it. If $C = 0$, keep the qubit (output the qubit to party).
3. If $C = 1$,
   a) Query $\mathcal{O}_v$, get v.
   b) If $v \neq i$
      i. Wait for the reception of x_i.
      ii. If $x_i = 0$, perform a Hadamard operation on the qubit. If $x_i = 1$, perform a $\sqrt{X}$ operation on the qubit.
      iii. Measure in the $\{|0\rangle, |1\rangle\}$ basis.
      iv. Send the outcome y_i to the Verifier via the classical channel resource.
   c) If $v = i$
      i. Create a random bit string $X = \{x_i\}_{i=1}^n$ with $x_i \in \{0, 1\}$ such that $\sum_{i=1}^n x_i \equiv 0 \pmod 2$
      ii. Send x_i it to party i via a classical channel resource, keep x_v.
      iii. Follow steps (iii).b.2 to (iii).b.4 and get y_v
      iv. Wait for the reception of all the other y_i.
      v. Upon the reception of all the y_i, output 0 to all if

$$\sum_{i=1}^{n} y_i \equiv \frac{1}{2} \sum_{i=1}^{n} x_i (\text{mod } 2)$$

      and 1 otherwise.

The actual verification protocol is thus seen here as a subroutine (steps (iii).(a) to (iii).(c)). All parties start by collectively querying a qubit and C and then, depending on the value of C, they either keep the qubit or do the verification protocol. During the verification protocol, one party is chosen to be the Verifier and after some classical communication and local quantum operations, the Verifier sends the output b_{out} to all parties.

The last converter, π_S, represents the local operation that an honest source would perform using the source to create an n-qubit GHZ state and send it to the parties. We consider a source separated from the parties, hence having its own converter. π_S simply consists in, upon receiving a signal from the parties, sending a classical description of the GHZ state to the $\mathcal{SG}_n$ resource. It implies that the source is not watching the classical communication between the parties at any point. Functioning like a filter,

this converter is made to be removed in case the source is noisy or some malicious party takes control of the source to reveal new interfaces to the outside world.

Protocol for the source π_S

1. Upon reception of a query by the parties, send a classical description of the GHZ state to the $\mathcal{SG}_n$ resource.

Together with $\mathcal{R}$, this completes the definition of the concrete multipartite entanglement resource $\pi_{[n]}\mathcal{R}\pi_S$ (see Fig. 3.11 for a 3-party example), which takes as input a start signal and outputs a bit C then a qubit from a GHZ state to each party or a bit $b_{out} = 0$.

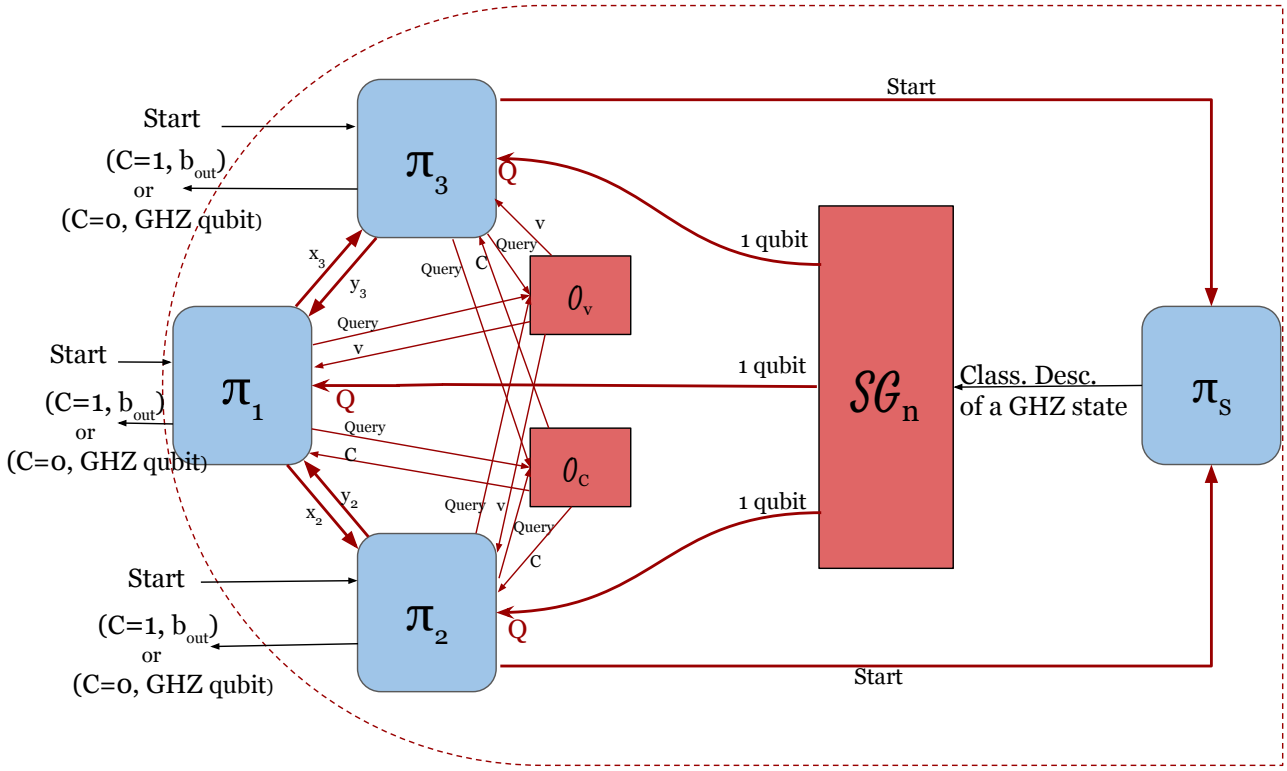


Figure 3.11: The $\pi_{[n]}\mathcal{R}\pi_S$ Resource within the dotted red line for $n = 3$ parties wishing to test a source, when party 1 is chosen to be the Verifier. We represent resources in red and converters in blue. We recall the timeline of the protocol: (1) all the parties π_i send a start signal to the source π_S that sends a classical description of a GHZ state to the $\mathcal{SG}_n$ resource. (2) Upon reception of the qubit, parties send a query to $\mathcal{O}_C$ and get C. (3) If $C = 0$ they output a GHZ qubit and if $C = 1$ they query $\mathcal{O}_v$ and get v (here party 1). (4) The Verifier sends instructions $X = \{x_i\}_{i=1}^n$ (here $\{x_2, x_3\}$) to others parties, get outcomes $Y = \{y_i\}_{i=1}^n$ (here $\{y_2, y_3\}$) and computes and broadcasts b_{out}. To avoid overloading the figure we don't represent quantum memories as well as the classical signals going from π_1 to π_S. As π_S represents honest behaviour from the source, we also don't represent the leakage of information from the classical channels.

3.2.3 Security Analysis

We come now to the proof of the main claim of this work, namely that the multipartite entanglement verification protocol π securely constructs the $\mathcal{MEV}_C$ resource out of $\mathcal{R}$. We proceed as expected from the security definition of Sec. 3.1.3 that is by finding simulators to emulate local dishonest behaviour on the ideal resource. A dishonest behavior from a party is simply modeled by removing the associated converter. This creates new free interfaces on the concrete resource accessible to a distinguisher. Simulators should render the ideal resource indistinguishable from dishonest concrete resources.

We will only consider cases that are of interest for our security claim which are when all parties are honest and when the source is noisy or malicious. The case of dishonest parties possibly tampering the source is discussed in Sec. 3.3.2, but it appears that composable security cannot be proven in the AC framework when a party is dishonest. Distinguishers in this section are all powerful, both classically and quantumly.

3.2.3.1 Correctness.

The first step of the proof corresponds to the correctness of the multipartite entanglement verification protocol, meaning that when all parties are honest and the source is honest the parties all get either a qubit from a GHZ state or a bit $b_{out} = 0$.

Theorem 3.1. *The multipartite entanglement verification protocol emulates the filtered ideal resource* $\mathcal{MEV}_C\perp$.

Proof. Let $\mathbf{D}$ be an all powerful distinguisher trying to guess between $\mathcal{MEV}_C\perp$ and $\pi_{[n]}\mathcal{R}\pi_S$. Let us look at the distribution of outputs that it will get from them.

$\mathbf{D}$ first sends start signals to both resources. When interacting with $\mathcal{MEV}_C\perp$, it gets $C = 1$ and $b_{out} = 0$ with some probability $1 - p$ and $C = 0$ and n qubits from a GHZ state with probability p. Throughout this work, the probability distribution of p is tuned to match the one of $\mathcal{O}_C$. When interacting with $\pi_{[n]}\mathcal{R}\pi_S$, the distinguisher thus performs the concrete multipartite entanglement verification protocol with the same probability p. If all parties share a GHZ, the condition $\sum_{i=1}^{n} y_i \equiv \frac{1}{2}\sum_{i=1}^{n} x_i (\mathrm{mod}\ 2)$ is always fulfilled (see [85] for complete proof). So the Verifier always sends $b_{out} = 0$ at the end. Hence, $\mathbf{D}$ gets $C = 1$ and $b_{out} = 0$ with probability $1-p$ and $C = 0$ and n qubits from a GHZ state with probability p.

We can conclude that for any distinguisher $\mathbf{D}$, $d^{\mathbf{D}}(\pi_{[n]}\mathcal{R}\pi_S, \mathcal{MEV}_C\perp) = 0$ hence

$$\pi_{[n]}\mathcal{R}\pi_S \approx \mathcal{MEV}_C\perp. \tag{3.5}$$

■

3.2.3.2 Dishonest source.

Let us now look at the case of a dishonest or noisy source. As custom in AC, we model this by removing the filter $\perp$ of the ideal resource and the protocol π_S of the concrete one (see Fig. 3.13). This leaves a new interface free for a distinguisher to send in a classical description of a state ρ. Because we do not use private but rather authenticated classical communication, the distinguisher also receives all leakage of classical communication between the parties and when they query oracles.

In order to prove security, as expected from the security definition of Sec. 3.1.3, we need to find a simulator σ_S such that we can prove $\pi_{[n]}\mathcal{R} \approx \mathcal{MEV}_C\sigma_S$. It should simulate the dishonest behaviour of the source watching over the classical communication of the parties. More specifically, it should emulate on the ideal resource the new interfaces a distinguisher has access to when π_S is unplugged from the concrete resource.

Let σ_S be the simulator shown in Fig. 3.12. It first takes as input a start signal from the $\mathcal{MEV}_C$ resource, then emulates the verification protocol by forwarding this start signal. After receiving a classical description of a state ρ, it forwards it to $\mathcal{MEV}_C$. It gets and forwards the bit C. If $C = 1$, it creates a random $v \in [n]$ and a random bit string $X = \{x_i\}_{i=1}^n$ such that $\sum_{i=1}^n x_i \equiv 0 \pmod 2$ and sends them to the outside world, except for x_v. Then it computes a table of possible measurement outcomes by calculating all necessary scalar products:

(3.6)

$$\begin{aligned} Pr[y_1 = 0, y_2 = 0, ..., y_n = 0] &= \langle 00...0 | \, U\rho U^\dagger \, | 00...0 \rangle \\ Pr[y_1 = 0, y_2 = 0, ..., y_n = 1] &= \langle 00...1 | \, U\rho U^\dagger \, | 00...1 \rangle \\ &... \\ Pr[y_1 = 1, y_2 = 1, ..., y_n = 1] &= \langle 11...1 | \, U\rho U^\dagger \, | 11...1 \rangle \end{aligned}$$

with $U = H^{x_1}(\sqrt{X})^{1-x_1} \otimes H^{x_2}(\sqrt{X})^{1-x_2} \otimes ... \otimes H^{x_n}(\sqrt{X})^{1-x_n}$ corresponding to the local operations made by each party on their qubit in the verification protocol. Then it randomly samples $Y = \{y_i\}_{i=1}^n$ from this table and sends them to the outside world, except for y_v.

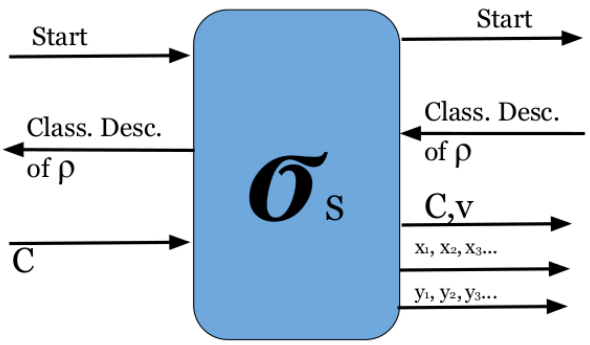


Figure 3.12: Simulator σ_S for a dishonest source.

Roughly speaking, σ_S classically emulates the whole multiparty protocol by reproducing the classical communication and local quantum operations. Plugged in $\mathcal{MEV}_C$, this defines a new resource $\mathcal{MEV}_C\sigma_S$ (see Fig. 3.14). With this simulator we can state that:

Theorem 3.2. *The multipartite entanglement verification protocol with a noisy or malicious source emulates the ideal resource $\mathcal{MEV}_C\sigma_S$.*

Proof. In this scenario, we have to prove an equivalence between $\mathcal{MEV}_C\sigma_S$ and $\pi_{[n]}\mathcal{R}$ (i.e., Figs. 3.13 and 3.14). This is done by showing that no distinguisher sending inputs and receiving outputs from both can guess which resource it is interacting with. In the concrete setting this means that the parties will share a state ρ that is τ-close to the GHZ state, with $\tau = \mathrm{TD}(|GHZ\rangle\langle GHZ|, \rho)$, that they will either keep or verify with probability S. In [85], it is shown that a state ρ passes the verification test with probability $1 - \frac{\tau^2}{2}$.

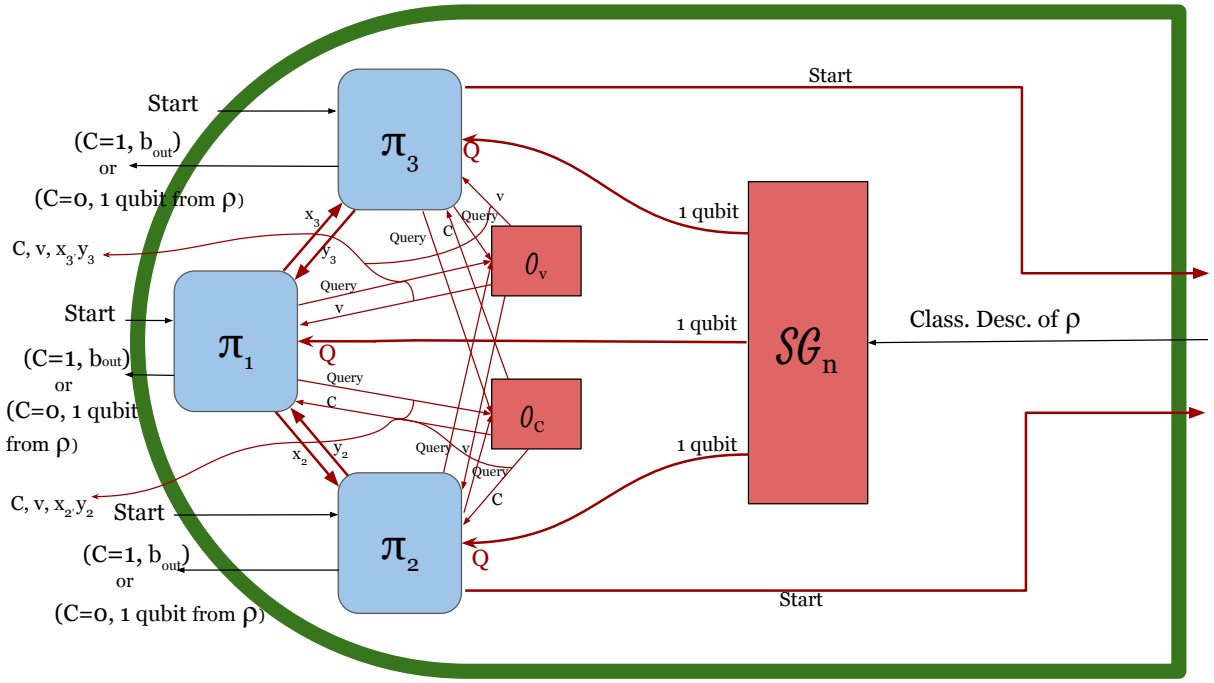


Figure 3.13: The $\pi_{[n]}\mathcal{R}$ resource for $n = 3$ parties when party 1 is chosen as the Verifier, accessed by a distinguisher (in green). To not overload the figure we join all leakages interfaces from the classical channel resources into two arrows, but they should each be considered as a different interface the distinguisher has access to.

Let **D** be an all powerful distinguisher trying to guess between $\pi_{[n]}\mathcal{R}$ and $\mathcal{MEV}_C\sigma_S$. In the concrete setting, it sends in start signals at the parties interfaces then receives it at the source interface. It then sends a classical description of a state ρ to $\mathcal{SG}_n$. **D** then sees all the classical communication happening out of the authenticated classical channels. More explicitly it will first see a bit C. If $C = 0$, it will see nothing but the qubits of ρ at each party's interface. If $C = 1$, a random identifier $v \in [n]$ leaks, then random bits $X\backslash\{x_v\}$ from the Verifier to each party. Then the outcome of each party's measurement except the Verifier's $Y\backslash\{y_v\}$ leaks and finally the bit b_{out} is broadcasted by the Verifier.

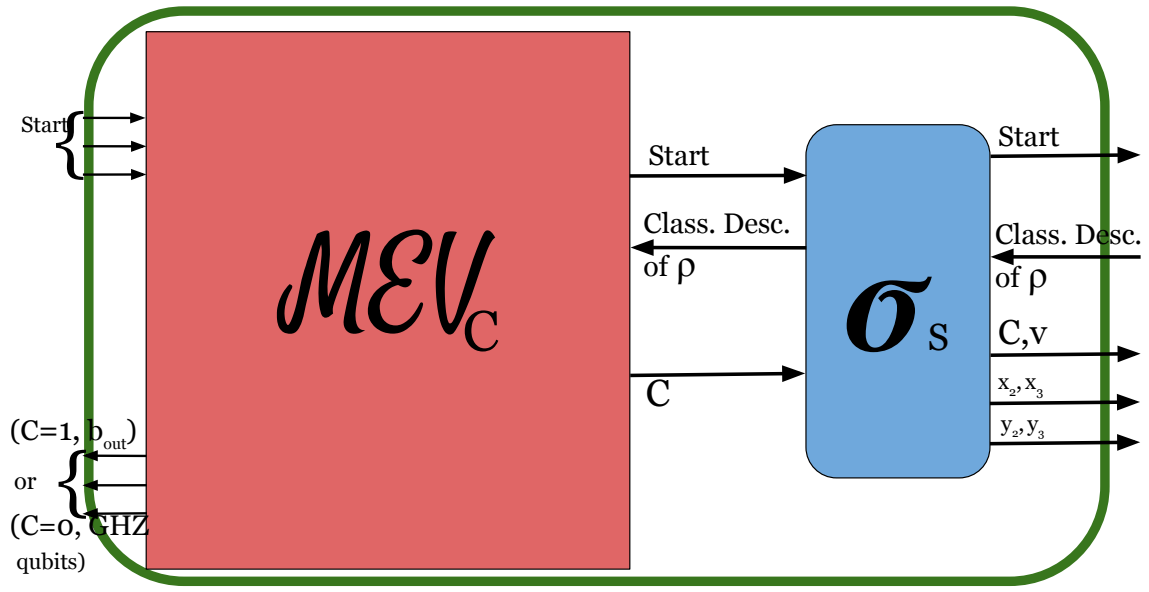


Figure 3.14: The $\mathcal{MEV}_C\sigma_S$ resource for $n = 3$ parties accessed by a distinguisher (in green).

In the ideal setting, after $\mathbf{D}$ sends in a start signal, $\mathcal{MEV}_C$ forwards it to σ_S. The simulator then sends a start signal simulating the query of a state by the parties. After that, the distinguisher sends a classical description of a state ρ to σ_S who forwards it to $\mathcal{MEV}_C$, which outputs C at all its interfaces. σ_S gets C and outputs it at its outside interface. If $C = 0$, $\mathcal{MEV}_C$ outputs the qubits of ρ at each party's interface. If $C = 1$, σ_S creates and outputs a random $\hat{v} \in [n]$ then computes a random bit string $\hat{X} = \{\hat{x}_i\}_{i=1}^n$ such that $\sum_{i=1}^n \hat{x}_i \equiv 0 \pmod 2$. It sends them to the outside world, except for $\hat{x}_v$. After that, σ_S computes the table of Eq. (3.6) and randomly samples $\hat{Y} = \{\hat{y}_i\}_{i=1}^n$. It outputs them all to the outside world except for $\hat{y}_v$. Finally $\mathcal{MEV}_C$ outputs $\hat{b}_{out} = 0$ with probability $1 - \frac{\tau^2}{2}$ and $\hat{b}_{out} = 1$ otherwise.

The probability distribution of the bit C is designed to match the probability distribution given by the oracle $\mathcal{O}_C$. In the concrete setting v is chosen randomly among the players through a query to the oracle $\mathcal{O}_v$ so we have that for all $i \in [n]$, $\Pr[v = i] = \Pr[\hat{v} = i]$. $X = \{x_i\}_{i=1}^n$ and $\hat{X} = \{\hat{x}_i\}_{i=1}^n$ are both chosen randomly so their probability distribution is the same. $Y = \{y_i\}_{i=1, i\neq v}^n$ are the outcomes of the measurements of each qubit ρ by each party in the $\{|0\rangle, |1\rangle\}$ basis after doing the operation indicated by each x_i. The state after each party applied their operation is $U\rho U^\dagger$ with $U = H^{x_1}(\sqrt{X})^{1-x_1} \otimes H^{x_2}(\sqrt{X})^{1-x_2} \otimes ... \otimes H^{x_n}(\sqrt{X})^{1-x_n}$. They are samples from the table of Eq. (3.6). Hence for each $i \in [n]$ we have that $\Pr[y_i = 0] = \Pr[\hat{y}_i = 0]$. Finally, by definition of our $\mathcal{MEV}_C$ resource, the probability distribution of $\hat{b}_{out}$ is the same as the one of b_{out}.

The probability distribution of the output given by the two resources depending on the inputs is thus the same. Hence we have that for any distinguisher $\mathbf{D}$, $d^{\mathbf{D}}(\pi_{[n]}\mathcal{R}, \mathcal{MEV}\sigma_S) = 0$ and

$$\pi_{[n]}\mathcal{R} \approx \mathcal{MEV}_C\sigma_S. \tag{3.7}$$

■

3.2.3.3 Conclusion.

We have proved that $\pi_{[n]}\mathcal{R}\pi_S \approx \mathcal{MEV}_C\perp$ and that $\exists\sigma_S$ s.t. $\pi_{[n]}\mathcal{R} \approx \mathcal{MEV}_C\sigma_S$. This means that the multipartite entanglement verification protocol presented is composable when all parties are honest but with a possibly dishonest source. The protocol can thus be thought of as a black box and equivalently replaced by the $\mathcal{MEV}_C$ resource (Fig. 3.5) when designing protocols using this one as a subroutine. It assumes that the parties have access to resources $\mathcal{R}$, including common oracles and quantum memories.

3.2.4 Application : Verified GHZ sharing resource.

The composability result we proved allows n parties to securely compose the protocol with itself multiple times. If the probability that $C = 0$ is sufficiently small, the protocol will be repeated on expectation enough rounds to allow the parties to build high confidence on the source's ability to create a state close to the GHZ state. Since the round where they will actually use the qubits sent by the source to perform some communication or computation protocol is unknown to the source, it is not possible for the source to adapt and decide when to send faulty states. Hence it forces the source to send states that are sufficiently close to the GHZ state every time it is queried. We call this protocol the multi-round multipartite entanglement verification protocol.

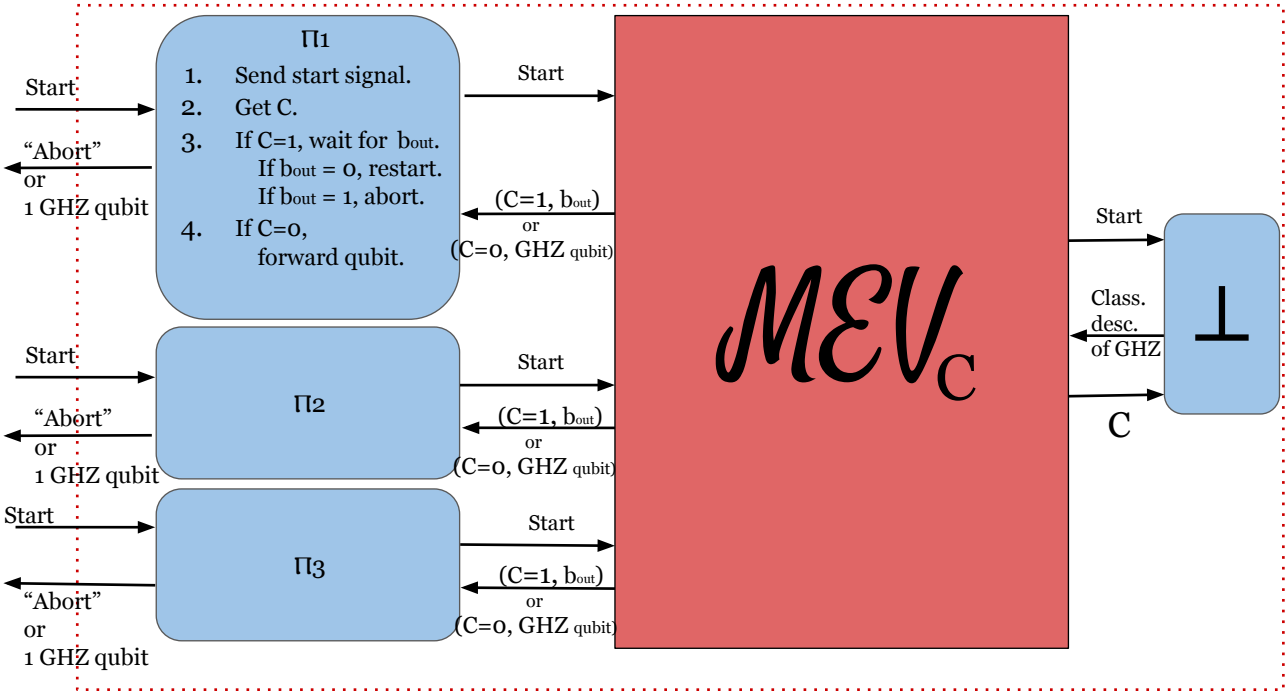


Figure 3.15: Multi-round verification resource $\Pi_{[n]}\mathcal{MEV}_C\perp$ for 3 parties (in the red dotted square). It takes start signals as input and outputs either a shared quantum state ϵ-close to the GHZ state or an abort signal.

By defining converters $\{\Pi_i\}_{i=1}^n$ representing the aforementioned protocol, we can construct a resource $\Pi_{[n]}\mathcal{MEV}_C\perp$ that gives either a state at least ϵ-close to the GHZ state to n parties or an abort signal (see Fig. 3.15 for a 3-party example and the explicit description of a Π_i). As it is a composable framework, AC allows us to state that

$$\Pi_{[n]}\pi_{[n]}\mathcal{R}\pi_S \approx \Pi_{[n]}\mathcal{MEV}_C\perp \tag{3.8}$$

$$\text{and } \exists\sigma_S \text{ s.t. } \Pi_{[n]}\pi_{[n]}\mathcal{R} \approx \Pi_{[n]}\mathcal{MEV}_C\sigma_S. \tag{3.9}$$

Let us define a *verified ϵ-GHZ state sharing* resource that we call $\mathcal{GHZ}$ (see Fig. 3.16). This resource is the idealisation of multipartite entanglement verification achieved through an interactive protocol between the source and the parties. We assume that at each round of the interaction a state is produced and shared by the source and the parties perform some verification protocol until, in the end, they decide to trust that the shared state is close to the GHZ state or abort the protocol. $\mathcal{GHZ}$ takes as input start signals from the parties, then interacts with the source and finally outputs either a state ϵ-close to the GHZ state or an abort signal. The interaction is abstractly modeled in the following way: first a Start signal is sent to the source interface, which replies with the classical description of a state ρ. Then $\mathcal{GHZ}$ will either ask for another state by sending a "Continue" signal to the source interface, or output an "Abort" signal to all interfaces because the current state was found to be far from the GHZ state, or, last, stop the protocol and share the last state it has received to the parties interface and send a "Stop" signal to the source interface. The probability that $\mathcal{GHZ}$ either asks for more states or outputs qubits can be tuned freely.

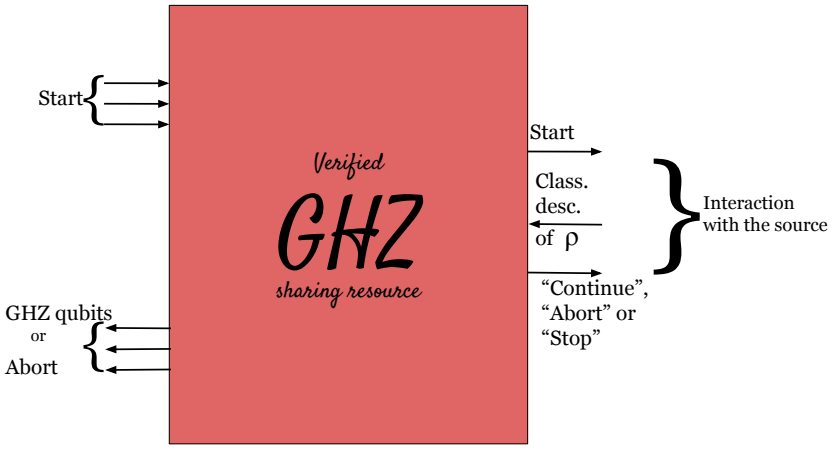


Figure 3.16: Verified ϵ-GHZ sharing resource for 3 parties. It takes start signals as input from the parties on the left interface then interacts with the source on the right interface. It outputs either a shared quantum state ϵ-close to the GHZ state or an abort signal to the parties.

This resource abstracts all the local operations and communication between the parties. From their point of view it is simply a source of states that are close to the GHZ state. However, to capture possibly malicious behavior from the source, we include the interaction on the source interface. We argue this is an abstract enough resource that captures all interactive verification procedures where the parties verify a number of states from the source before asserting that the source gives close to GHZ states.

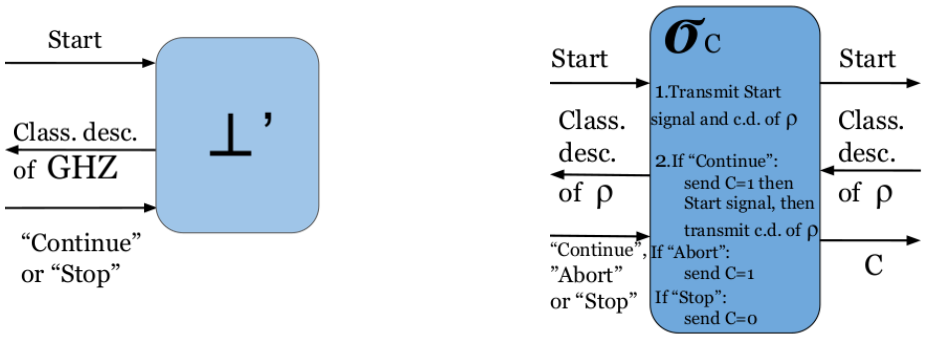


Figure 3.17: Filter $\perp'$ (on the left) and simulator σ_C (on the right) to plug into the $\mathcal{GHZ}$ resource. The former represents the honest use of the resource and allows us to state the correctness of the AC security proof (Eq. (12)). The latter is the simulator that models the interface to which a distinguisher has access when we consider the source to act maliciously using the multiround multipartite entanglement verification resource $\Pi_{[n]}\mathcal{MEV}_C$. It allows us to derive the second part (noisy or malicious source) of the AC security proof (Eq. (13)).

Similarly to Sec. 3.2.3, when we define $\perp'$ and σ_C as in Fig. 3.17, we can prove that

$$\Pi_{[n]}\mathcal{MEV}_C\perp \approx \mathcal{GHZ}\perp' \tag{3.10}$$

$$\text{and } \Pi_{[n]}\mathcal{MEV}_C \approx \mathcal{GHZ}\sigma_C \tag{3.11}$$

Hence,

$$\Pi_{[n]}\pi_{[n]}\mathcal{R}\pi_S \approx \mathcal{GHZ}\perp \tag{3.12}$$

$$\text{and } \exists\sigma_S \text{ s.t. } \Pi_{[n]}\pi_{[n]}\mathcal{R} \approx \mathcal{GHZ}\sigma_S \tag{3.13}$$

This means that the multi-round multipartite entanglement verification protocol constructs the $\mathcal{GHZ}$ resource out of $\mathcal{R}$. We can also state that it is composably secure in the setting of all honest parties and in the presence of a possibly malicious or noisy source. We can conclude that this protocol allows n parties to get a GHZ state as a subroutine of a bigger protocol with an untrusted source.

3.3 Discussion

3.3.1 Case of honest parties

The multipartite entanglement verification protocol is particularly suited in a distributed computing scenario where the parties are honest but where there could be a faulty resource. They can use this protocol to check if the noise of an entanglement source is small enough for practical use. Indeed, if after many rounds of performing this protocol the output is most of the time $b_{out} = 0$, they can realistically be sure that the source is producing states that are close to the GHZ state. Its composability allows for the construction of the multi-round verification resource, which can find practical use in larger communication protocols, as for example in anonymous ranking [119], quantum secret sharing [120] or

distributed consensus [121] protocols. In fact, any protocol that starts with a GHZ state shared among n honest parties that don't trust their source can be composed with this one in a secure way. This might seem limiting but is in fact realistic in many distributed computing settings.

This protocol can also be seen as a building block of a quantum network. We can reasonably assume that parties are honest when performing protocols establishing the network in the same way we think about parties when considering entanglement distillation, network or transport layer protocols of the OSI model of the classical Internet. An intermediate scale metropolitan quantum Internet example is a network where a source shares a GHZ state to all parties at each time-step, that they either use or verify. Our verification protocol can in this case be hidden in the assumptions of the network. Moreover recent work on graph state verification [122] hint that composable security can be extended to verification of any graph state. This is particularly relevant because not all states can be obtained from local operations on the GHZ state and classical communications (see e.g.[123]).

One may wonder why we did not start by defining the multi-round and the verified ϵ-GHZ sharing resources of the above section from the beginning. This is indeed the practical resource that one would like to use in larger protocols as it directly provides quantum states that are ϵ-close to the GHZ state. This was based on the fact that our priority was not to define *ad hoc* the most useful resource, but to succeed in modeling a resource that is as close as possible to the signals that will actually be sent by the parties when performing the protocol in real life, and use this resource in a composably secure way to obtain a practical multipartite entanglement verification resource, that of the multi-round resource. Our one-round resource captures the important parameters for composing the protocol in larger routines and it allows for modularity and a more precise understanding of what happens in the multi-round case. Moreover, the composability of the one-round GHZ-verification protocol allows to perform many of these multi-round GHZ-verification protocols in parallel. By sending start signals to different sources, a group of honest parties could decide which source provides the best quantum states. This allows this protocol to fit in a bigger network model where the parties could get states from different sources.

We will also see below that dishonest behavior of a party already causes composability issues in the one-round case thus we get a better understanding of the issues by proving composability in this case. Moreover the box-shaped resource that we construct using AC (Fig. 3.7) is close to the black-box picture that one would like to have when thinking of the building blocks of near-term Quantum Internet applications such as the one listed above [93, 119, 120, 121]. Finally, we emphasize that this protocol only assumes classical communications between the parties and single-qubit local operations for each party, making it a good candidate for scalable application development.

3.3.2 Case of a malicious party

When studying this problem, it is natural to think about the case of dishonest parties possibly controlling the source. If we assume that dishonest parties are trying to make the others accept a state that is not close the GHZ state, results from [85] and [86] show that for one round of verification, the output bit b_{out} depends on the minimal distance between the GHZ state and the shared state up to local operations on the part of the state held by the dishonest parties. This result holds even when the dishonest parties have

complete control over the state generation resource. For this to hold, we have to assume that the Verifier is always honest and that the parties cannot influence the probability distributions of the oracles $\mathcal{O}_C$ and $\mathcal{O}_v$.

Yet as discussed in the first part of this chapter, it seems that this protocol cannot be proven composable in the Abstract Cryptography framework when considering a dishonest party. Indeed one straightforward strategy for a dishonest party would be to make the protocol abort randomly, which would give false information about the source. Any dishonest party actually has complete control on the distribution of the concrete resource's output b_{out} while the ideal resource's output is fixed by the distance with the GHZ state of the state given as input. Even if we add switches to our resource on which a simulator could act to make it abort (as custom is such cases), we could not reproduce the abort probability distribution of our concrete protocol in the ideal world. It seems impossible to find a simulator that emulates the interfaces a distinguisher has access to when removing one of the π_i. This can be seen in the AC framework by removing the converters corresponding to the dishonest parties and finding distinguishing attacks for every possible simulator. We would moreover need extra assumptions on the quantum registers and the access to the multiparty computation oracles $\mathcal{O}_C$ and $\mathcal{O}_v$ that seem unpractical in a near-term network.

However, our composability result comes on top of the security proof of [85] meaning that our multiparty entanglement verification protocol is secure against possible coalition of dishonest parties and source trying to persuade others that they share a GHZ when they don't and composably secure against a malicious source. It does not limit the use of our protocol to the all honest case. No attack is known to make use of the repetition of the protocol that would alter the *integrity* of the shared state more than simply repeating the attack described in [85]. On the other hand, the *availability* of the resource can be compromised by dishonest behaviour in an unpredictable way. This sheds light on the pros and cons of using a game-based framework versus a composable framework. In the former we can restrict dishonest behaviour to specific attacks and get specific security properties while in the former we can only act on how powerful the class of distinguishers is but get more general security claims. By studying the protocol in different frameworks, we are able to take the best of all approaches and show different aspects of security that increase confidence in the protocols.

3.3.3 Practical implementation in a near-term quantum network

To actually implement the protocol, one has to replace the resources in $\mathcal{R}$ with actual protocols or physical resources. Multiparty classical protocols should take the place of oracle calls, and have to be proved composable to securely construct $\mathcal{R}$ out of them and the quantum resources. An example of a protocol replacing calls to $\mathcal{O}_C$ is the random bit protocol explicited in [93] and [124]. Previous work [85] shows that by choosing the probability of using the qubit for computation ($C = 0$) to be $\frac{\epsilon^2}{4n\delta}$ for some $\delta > 0$, all honest parties have the guarantee that the probability the state used has distance at least ϵ from the correct one is at most $\frac{1}{\delta}$.

Qubit transportation should be taken care of by physical channels and protocols that one has to study to see if they are equivalent to the quantum channel resource presented in this work. This would

happen at the equivalent of the link layer of the OSI model for the Quantum Internet. As previously mentioned, any noisy channel can be modeled by a perfect channel in which a noisy state is given as input, and a noisy source can be modeled by a perfect source in which a classical description of a noisy state is given. The $\mathcal{SG}_n$ resource is designed as an attempt to capture what happens in the most general case when the protocol is performed in the lab where, at some point, a classical signal is sent to a quantum device that creates a state. Usually some information is accessible to the person controlling the device to check (for example by heralding photons) if the right state has been created. We suppose here that none of this information leaks from $\mathcal{SG}_n$ as it is the more restricting scenario. Moreover we don't restrict the source to create only n-qubit states, but merely enforce that it is able to create states up to this size. The proof holds even if the source creates bigger states and keeps part of it or sends it to a malicious party. $\mathcal{SG}_n$ is thus not meant to be realistic but to give an abstract embodiment of any source. A photonic implementation of a loss-tolerant variation of the original protocol has been achieved with 4 parties [86]. This leads to expect near-term realization of our protocol, presenting all security properties as well as composability and modularity for use in bigger protocols.

Lastly, the quantum memory assumption can be removed by asking the parties to measure their bit directly after receiving it and flipping the outcome randomly depending on the input given by the Verifier. We would lose the security properties against a malicious party from [85] that are based on the actual order of the inputs for each party. In our all honest setting, this would not matter so this protocol can actually be used in near-term architecture to securely check a source. Experimental realization of this protocol in a composable way is currently studied, which would allow to take this protocol as a concrete building block for applications in the quantum Internet. Whether this protocol should remain in the application layer or be hidden in some network or transport layer is still to be determined and will depend on future developments in quantum network architectures.

3.3.4 Thoughts on composable security and Abstract Cryptography

This work was done in the first years of my thesis research and the conclusion was not very satisfactory. For a long time, we considered that composable is a too restrictive notion with very little actual practical use. Consequently we dropped this topic for a while. However, we recently started questioning the methodology of the proof for multi-party protocols. It seemed that a strong assumption that we considered as essential can actually be lifted. Namely, when considering multiple dishonest parties and designing simulators to emulate the free interfaces accessed by a distinguisher, we restricted ourselves to local simulators. This means that simulators should not interact because the communication between them would involve new resources that were not considered in the construction of this ideal resource. This is the main cause for not being able to design a set of simulators that would be able to simulate dishonest behaviour from a party possibly colluding with the source.

After some discussions with U. Maurer and R. Renner, it seems that the Abstract Cryptography framework has now evolved towards removing of the concept of simulators and that our restriction on the simulator does not necessarily hold. Adding resources to allow communication between the different simulators should be possible without affecting the composability proof. They however have to

be clearly stated in the description of the ideal resource. With Léo Colisson, we will work on studying the composable security of a more general protocol, namely generic graph-state verification, in this new context.

When designing protocols for the future Quantum Internet, composable security is a very useful property. A protocol that is proven composably secure can be used as a building block for bigger and more complex protocols without having to prove security again. It is however quite a demanding property for an actual implementations of the protocol. Composable security relies on many assumptions: all the resources used in the concrete version of the protocol have to be actually realisable and proven composable. In the context of noisy quantum communication with error correction protocol on top of each data transfer this could cause flaws in the concrete representation of the protocol. Classical communication and multiparty computation should also be proven composable. However, research that we discovered after this work shows that multi-party classical computation has been proven composable in the Universal Composability framework [125]. Hence, studying the composable security of protocols could yield interesting results, but it is however not clear yet if they will have practical use on actual implementations of quantum network protocols.

Chapter 4

Quantum Repeaters

In this chapter, we take a close look at communication between two nodes through an optical fiber which is a crucial building block of quantum networks. Unfortunately, after a few tens of kilometers, photon loss in fiber becomes predominant and prevents practical applications. The well known PLOB bound [22] gives fundamental limits on quantum communication over long distance in a fiber. Moreover the no-cloning theorem prevents us from simply copying a quantum state and resending it before it is lost. One way to overcome this issue is to use quantum repeaters, analogs of amplifiers in a classical network. A quantum repeater is the combination of a protocol and some devices that allow quantum communication over a longer distance than what would be achievable with a direct fiber link. It typically divides a long-distance link between two nodes into sublinks of smaller length.

Contribution and outline: In this chapter, we study four different repeater schemes based on NV-center nodes. We notably investigate the strategy of establishing a cut-off on the number of trials in establishing entanglement in one sublink before moving on to the next. We model and simulate the secret key rate of the four schemes in the context of quantum key distribution. This work was done in collaboration with Filip Rozpedeck and Kenneth Goodenough, who participated in writing what follows. In Section 4.2 we discuss and detail the different repeater proposals that will be assessed in this work. In Section 4.3 we expand on how the different components of the repeater proposals would be implemented experimentally. Section 4.4 details how to calculate the secret-key rate achieved with the quantum repeater proposals from the modeled components. In Section 4.5 we discuss how to assess the performance of a quantum repeater. The comparison of the different repeater proposals is performed in Section 4.6, which allows us to conclude with our results in Section 4.7. The numerical results of this work were produced with a Python and a Mathematica script.

Article Link: The full article can be found at https://arxiv.org/abs/1809.00364 and is published in Physical Review A (Phys. Rev. A 99, 052330, May 2019)

4.1 Introduction

One of the main hurdles for long-distance quantum communication is the *loss* of photons, whether it is through fiber or free-space. Unfortunately, the no-cloning theorem [126] makes the amplification of the transmitted quantum states impossible. For tasks such as the generation of shared secret key or entanglement, this limits the corresponding generation rate to scale at best linearly in the transmissivity η of the fiber joining two distant parties [127, 128, 129].

Luckily, while quantum mechanics prevents us from overcoming the effects of losses through amplification, it is possible to do so using repeater stations [130, 131, 132]. Formally, we call a quantum repeater a device that allows for a better performance than can be achieved over the direct communication channel alone [23]. This performance is measured differently for different tasks, such as secret-key generation or transmission of quantum information. Consequently, the optimal performance that can be achieved over the direct channel without using repeaters, called the channel capacity, is also different for these two tasks. Here we will assess our proposed repeater schemes for the task of secret-key generation, as it is easier to realize experimentally. Our formal definition of a repeater—as opposed to a relative definition with respect to some setup of reference—endows the demonstration of a quantum repeater with a fundamental meaning that cannot be affected by future technological developments in the field.

However, a successful experimental implementation of a quantum repeater has not yet been demonstrated. This is mainly due to the additional noise introduced by such a quantum repeater. The first demonstration of a functioning quantum repeater will form an important step towards practical quantum communication and the quantum internet [133].

A multitude of quantum repeater schemes have been put forward [134, 135, 136, 137, 138, 131, 139, 140], each with their own strengths and weaknesses. *A priori*, it is not clear which of those schemes will perform best with current or near-term experimental parameters. In this work we propose three such schemes and together with the fourth scheme analyzed before [141, 23], we assess their performance for generating secret key. We consider their implementation based on nitrogen-vacancy centers in diamond (NV centers), a system which has properties making it an excellent candidate for long-distance quantum communication applications [142, 11, 10, 143, 144, 145, 146, 147, 148, 149].

The four considered schemes are: the "single sequential quantum repeater node" (first proposed and studied in [141], then further analyzed in [23]), the single-photon scheme (proposed originally in the context of remote entanglement generation [150], also studied in the context of secret-key generation without quantum memories [54]), and two schemes which are a combination of the first two. See Fig. 4.1 for a schematic overview of the repeater proposals considered in this work.

We compare the *secret-key rate* of each of these schemes to the highest theoretically achievable secret-key rate using direct transmission, the *secret-key capacity of the pure-loss channel* [129]. We show that one of these schemes, the *single-photon scheme*, can surpass the secret-key capacity by a factor of seven. This shows the viability of this scheme for the first experimental implementation of a quantum repeater.

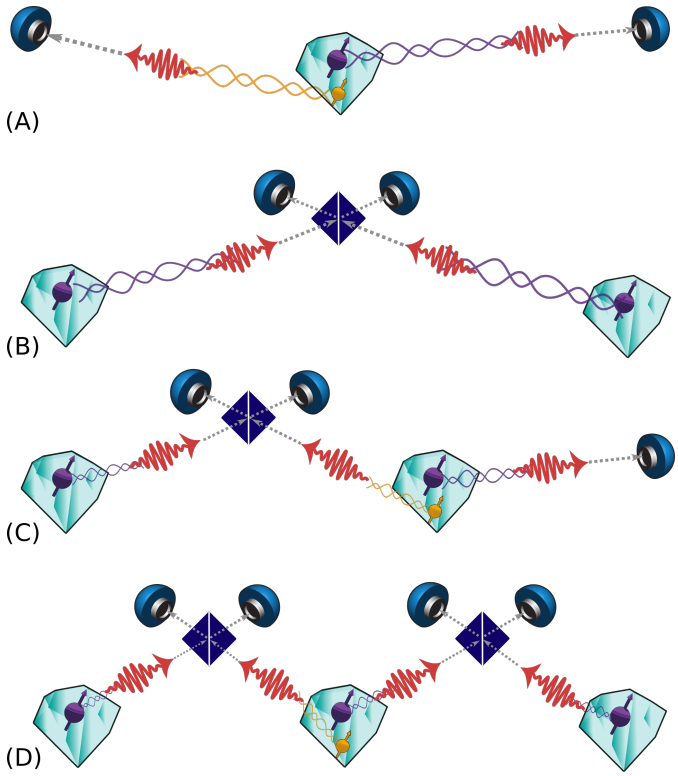


Figure 4.1: (Color on-line) Schematic overview of the four quantum repeater schemes assessed in this work. From top to bottom: the Single Sequential Quantum Repeater (SiSQuaRe) scheme (A), the single-photon scheme (B), the Single-Photon with Additional Detection Setup (SPADS) scheme (C) and the Single-Photon Over Two Links (SPOTL) scheme (D). The purple particles represent NV electron spins capable of emitting photons (red wiggly arrows) while the yellow particles represent carbon ^{13}C nuclear spins. Dark blue squares depict the beam splitters used to erase the which-way information of the photons, followed by blue photon detectors. For more details on the different proposals, see Section 4.2.

4.2 Quantum repeater schemes

In the following section we present the quantum repeater schemes that will be assessed in this work. All these schemes use NV center based setups which involve memory nodes consisting of an electron spin qubit acting as an optical interface and possibly an additional carbon ^{13}C nuclear spin qubit acting as a long-lived quantum memory (see Sec. 1.1.3). Here, we briefly go over all the proposed schemes, motivate why they are interesting from an experimental perspective and discuss their advantages and disadvantages.

4.2.1 The Single Sequential Quantum Repeater (SiSQuaRe) scheme

The first scheme that we discuss here was proposed and analyzed in [141], and further studied in [23]. The scheme involves a node holding two quantum memories in the middle of Alice and Bob (see Fig. 4.2). This middle node tries to send a photonic qubit, encoded in the time-bin degree of freedom, that is entangled with one of the quantum memories, through a fiber to Alice. This is attempted repeatedly until the photon successfully arrives, after which Alice performs a BB84 [151] or a six-state measurement [152, 153].

By performing such a measurement, the quantum memory will be steered into a specific state depending on the measurement outcome. Now the same is attempted on Bob's side. After Bob has measured a photon, the middle node performs a Bell-state measurement on both quantum memories. Using the classical information of the outcome of the Bell-state measurement, Alice and Bob can generate a single raw bit. In our model, the middle node has only one photonic interface (corresponding to the NV electron spin), and hence has to send the photon sequentially firstly to Alice and then to Bob.

While trying to send a photon to Bob, the state stored in the middle node will decohere. A possible way to compensate for the effects of decoherence is to introduce a so-called *cut-off* [23]. The cut-off is a limit on the number of attempts we allow the middle node to try and send a photon to Bob. If the cut-off is reached, the stored state is discarded, and the middle node attempts again to send a photon to Alice. Since the scheme starts from scratch, we are effectively trading off the generation time versus the quality of our state. By optimizing over the cut-off, it is possible to considerably increase the distance over which secret key can be generated [23].

Setup and scheme

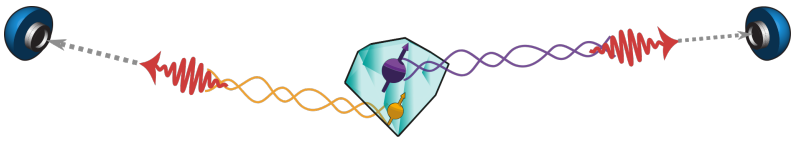


Figure 4.2: (Color on-line) Schematic overview of the SiSQuaRe scheme. The NV center in the middle first attempts to generate an entangled photon-electron pair, after which it tries to send the photon through the fiber to Alice. Alice then directly measures the photon, using either a BB84 or a six-state measurement. Then after the state of the electron spin is swapped to the carbon ^{13}C nuclear spin, the same is attempted on Bob's side. After both Alice and Bob measured a photon, a Bell-state measurement is performed on the two quantum states held by the middle node. Alice and Bob can use their measurement outcomes together with the outcome of the Bell-state measurement to generate a single raw bit of key.

We will now describe the exact procedure of this scheme, when Alice and Bob use a nitrogen-vacancy center in diamond as quantum memories and as a photon source. The scheme that we study is the following:

SiSQuaRe scheme

1. The quantum repeater attempts to generate an entangled qubit-qubit state between a photon and its electron spin, and sends the photon to Alice through a fiber.
2. The first step is repeated until a photon arrives at Alice's side, after which she performs a BB84 or a six-state measurement. The electron state is swapped to the carbon spin.
3. The quantum repeater attempts to do the same on Bob's side while the state in the carbon spin is kept stored. This state will decohere during the next steps.
4. Repeat until a photon arrives at Bob's side, who will perform a BB84 or a six-state measurement. If the number of attempts n reaches the cut-off n^*, restart from step 1.
5. The quantum repeater performs a Bell-state measurement and communicates the result to Bob.
6. All the previous steps are repeated until sufficient data have been generated.

4.2.2 The single-photon scheme

Cabrillo et al. [150] devised a procedure that allows for the heralded generation of entanglement between a separated pair of matter qubits (their proposal discusses specific implementation with single atoms, but the scheme can also be applied to other platforms such as NV centers or quantum dots) using linear optics. For the atomic ensemble platform this scheme also forms a building block of the DLCZ quantum repeater scheme [135]. Here we will refer to this scheme as a single-photon scheme as the entanglement generation is heralded by a detection of only a single photon. This requirement of successful transmission of only a single photon from one node makes it possible for this scheme to qualify as a quantum repeater (see below for more details).

The basic setup of the single-photon scheme consists of placing a beam splitter and two detectors between Alice and Bob, with both parties simultaneously sending a photonic quantum state towards the beam splitter. The transmitted quantum state is entangled with a quantum memory, and the state space of the photon is spanned by the two states corresponding to the presence and absence of a photon. Immediately after transmitting their photons through the fiber, both Alice and Bob measure their quantum memories in a BB84 or six-state basis (see the discussion of which quantum key distribution protocol is optimal for each scheme in Section 4.4.2 and in Section 4.6.1). Note that this is equivalent to preparing a specific state of the photonic qubit and therefore is closely linked to the measurement device independent quantum key distribution (see Sec.2.1.1.3) as discussed in Appendix A.9. However, preparing specific states that involve the superposition of the presence and absence of a photon on its own is generally experimentally challenging. The NV-implementation allows us to achieve this task precisely by preparing spin-photon entanglement and then measuring the spin qubit. Afterwards, by conditioning on the click of a single detector only, Alice and Bob can use the information of which detector clicked to generate a single raw bit of key, see Appendix A.5 and [150] for more information.

The main motivation of this scheme is that, informally, we only need one photon to travel half the distance between the two parties to get an entangled state. This thus effectively reduces the effects of losses, and in the ideal scenario the secret-key rate would scale with the square root of the total transmissivity η, as opposed to linear scaling in η (which is the optimal scaling without a quantum repeater [154]). However, one problem that one faces when implementing this scheme is that the fiber induces a phase shift on the transmitted photons. This shift can change over time, e.g. due to fluctuations in the temperature and vibrations of the fiber. The uncertainty of the phase shift induces dephasing noise on the state, reducing the quality of the state.

To overcome this problem, a two-photon scheme was proposed by Barrett and Kok [155], which does not place such high requirement on the optical stability of the setup. Specifically, in the Barrett and Kok scheme the problem of optical phase fluctuations is overcome by requiring two consecutive clicks and performing additional spin flip operations on both of the remote memories. The Barrett and Kok scheme has seen implementation in many experiments [156, 157, 158, 159]. However, the requirement of two consecutive clicks implies that a setup using only the Barrett and Kok scheme with two memory nodes will never be able to satisfy the demands of a quantum repeater. Specifically, the probability of getting two consecutive clicks will not be higher than the transmissivity of the fiber between the two parties and therefore will not surpass the secret-key capacity.

In the single-photon scheme, on the other hand, the dephasing caused by the unknown optical phase shift is overcome by using active *phase-stabilization* of the fiber to reduce the fluctuations in the induced phase. This technique has been used in the experimental implementations of the single-photon scheme for remote entanglement generation using quantum dots [160, 161], NV centers [142] and atomic ensembles [162]. For experimental details relating to NV-implementation, we refer the reader to Section 4.3. This phase-stabilization technique effectively reduces the uncertainty in the phase, allowing us to significantly mitigate the resulting dephasing noise, see Appendix A.1 for mathematical details.

In contrast to the Barrett and Kok scheme, the single-photon scheme cannot produce a perfect maximally entangled state, even in the case of perfect operations and perfect phase-stabilization. This is because losses in the channel result in a significant probability of having both nodes emitting a photon which can also lead to a single click in one of the detectors, yet the memories will be projected onto a product state. As we discuss below, this noise can be traded versus the probability of success of the scheme by reducing the weight of the photon-presence term in the generated spin-photon entangled state. This is discussed in more detail below and the full analysis is presented in Appendix A.5.

The single-photon scheme with phase-stabilization is a promising candidate for a near-term quantum repeater with NV centers. We note here that recently other QKD schemes that use the MDI framework have been proposed, for example Twin-Field QKD. These schemes, similarly to our proposal, use single-photon detection events to overcome the linear scaling of the secret-key rate with η [54, 163, 164]. In these proposals, in contrast to our single-photon scheme, no quantum memories are used, but instead Alice and Bob send phase-randomized optical pulses to the middle heralding station.

Setup and scheme

In the setup of the single-photon scheme Alice and Bob are separated by a fiber where in the center there is a beam splitter with two detectors (see Fig. 4.3). They will both create entanglement between a photonic qubit and a stored spin and send the photonic qubit to the beam splitter.

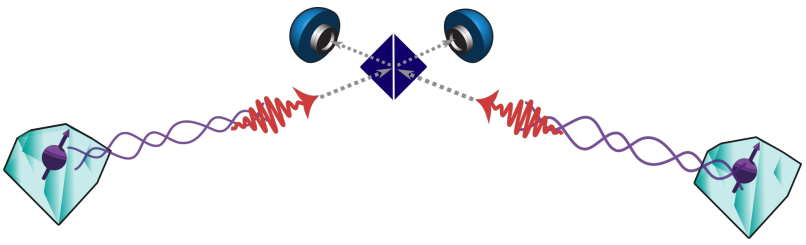


Figure 4.3: (Color on-line) Schematic overview of the single-photon scheme. Alice and Bob simultaneously transmit a photonic state from their NV centers towards a balanced beam splitter in the center. This photonic qubit, corresponding to the presence and absence of a photon, is initially entangled with the NV electron spin. If only one of the detectors (which can be seen at the top of the figure) registers a click, Alice and Bob can use the information of which detector clicked to generate a single raw bit of key.

Alice and Bob thus perform the following:

Single-click scheme

1. Alice and Bob both prepare a state $|\psi\rangle = \sin\theta\,|\downarrow\rangle\,|0\rangle + \cos\theta\,|\uparrow\rangle\,|1\rangle$ where $|\downarrow\rangle/|\uparrow\rangle$ refers to the dark/bright state of the electron-spin qubit, $|0\rangle/|1\rangle$ indicates the absence/presence of a photon, and θ is a tunable parameter.
2. Alice and Bob attempt to both separately send the photonic qubit to the beam splitter.
3. Alice and Bob both perform a six-state measurement on their memories.
4. The previous steps are repeated until only one of the detectors between the parties clicks.
5. The information of which detector clicked gets sent to Alice and Bob for classical correction.
6. All the previous step are repeated until sufficient data have been generated.

The parameter θ can be chosen by preparing a non-uniform superposition of the dark and bright state of the electron spin $|\psi\rangle = \sin\theta\,|\downarrow\rangle + \cos\theta\,|\uparrow\rangle$ via coherent microwave pulses. This is done before applying the optical pulse to the electron which entangles it with the presence and absence of a photon. The parameter θ can then be tuned in such a way as to maximize the secret-key rate. In the next section, we will briefly expand on some of the issues arising when losses and imperfect detectors are present. We show the full explanation and calculations in Appendix A.5.

Realistic setup

In any realistic implementation of the single-photon scheme, a large number of attempts is needed before a photon detection event is observed. Furthermore, a single detector registering a click does not necessarily mean that the state of the memories is projected onto the maximally entangled state. This is due to multiple reasons, such as losing photons in the fiber or in some other loss process between the emission and detection, arrival of the emitted photons outside of the detection time-window and the fact that *dark counts* generate clicks at the detectors. Photon loss in the fiber effectively acts as amplitude-damping on the state of the photon when using the presence/absence state space [129, 165]. Dark counts are clicks in the detectors, caused by thermal excitations. These clicks introduce noise, since it is impossible to distinguish between clicks caused by thermal excitations and the photons traveling through the fiber if they arrive in the same time-window. All these sources of loss and noise acting on the photonic qubits are discussed in detail in Appendix A.1. Finally we note that we assume here the application of non-number resolving detectors. This can lead to additional noise in the low loss regime, since then the event in which two photons got emitted cannot be distinguished from the single-photon emission events even if no photons got lost. However, in any realistic loss regime this is not a problem, since the probability of two such photons arriving at the heralding station is quadratically suppressed with respect to events where only one photon arrives. In the realistic regime, almost all the noise coming from the impossibility of distinguishing two-photon from single-photon emission events is the result of photon loss. Namely, if a two-photon emission event occurs and the detector registers a click, then with dominant probability it is due to only a single photon arriving, while the other one being lost. Hence the use of photon-number resolving detectors would not give any visible benefit with respect to the use of the non-number resolving ones. For a detailed calculation of the effects of losses and dark counts for the single-photon scheme, see Appendix A.5.

4.2.3 Single-Photon with Additional Detection Setup (SPADS) scheme

The third scheme that we consider here is the Single-Photon with Additional Detection Setup (SPADS) scheme, which is effectively a combination of the single-photon scheme and the SiSQuaRe scheme as shown in Fig. 4.4. If the middle node is positioned at two-thirds of the total distance away from Alice, the rate of this setup would scale, ideally, with the cube root of the transmissivity η.

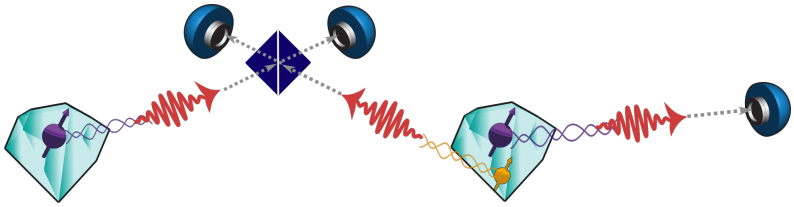


Figure 4.4: (Color on-line) Schematic overview of the SPADS scheme. First, the two NV centers run the single-photon scheme, such that Alice measures her electron spin directly after every attempt. After success, the middle node swaps its state to the carbon spin. Then the middle node generates electron-photon entangled pairs where the photonic qubit is encoded in the time-bin degree of freedom and sent to Bob. This is attempted until Bob successfully measures the photon or until the cut-off is reached. If the cut-off is reached, the scheme gets restarted, otherwise the middle node performs an entanglement swapping on its two memories and communicates the classical outcome to Alice and Bob, who can correct their measurement outcomes to obtain a bit of raw key.

This scheme runs as follows:

SPADS scheme

1. Alice and the repeater run the single-photon scheme until success, however, only Alice performs her spin measurement immediately after each spin-photon entanglement generation attempt. This measurement is either in a six-state or BB84 basis.
2. The repeater swaps the state of the electron spin onto the carbon spin.
3. The repeater runs the second part of the SiSQuaRe scheme with Bob. This means it generates spin-photon entanglement between an electron and the time-bin encoded photonic qubit. Afterwards, it sends the photonic qubit to Bob. This is repeated until Bob successfully measures his photon in a six-state or BB84 basis or until the cut-off n^* is reached in which case the scheme is restarted with step 1.
4. After Bob has received the photon and communicated this to the repeater, the repeater performs a Bell-state measurement on its two quantum memories and communicates the classical result to Bob.
5. All the previous steps are repeated until sufficient data have been generated.

The motivation for introducing this scheme is two-fold. Firstly, we note that by using this scheme we divide the total distance between Alice and Bob into three segments: two segments corresponding to the single-photon subscheme and the third segment over which the time-bin encoded photons are sent. This gives us one additional independent segment with respect to the single-photon or the SiSQuaRe scheme on its own. Hence, for distances where no cut-off is required, we expect the scaling of the secret-key rate with the transmissivity to be better than the ideal square root scaling of the previous two schemes. Furthermore, dividing the total distance into more segments should also allow us to reach larger distances before dark counts become significant. When considering the resources necessary to run this scheme, we note that the additional third node needs to be equipped only with a photon detection setup.

Secondly, we note that the SPADS scheme can also be naturally compared to the scenario in which an NV center is used as a single photon source for direct transmission between Alice and Bob. Both the setup for the SPADS scheme and such direct transmission involve Alice using an NV for emission and Bob having only a detector setup. Hence, the SPADS scheme corresponds to inserting a new NV-node (the repeater) between Alice and Bob without changing their local experimental setups at all. This motivates us to compare the achievable secret-key rate of the SPADS scheme and direct transmission. We perform this comparison on a separate plot in Section 4.6.

4.2.4 Single-Photon Over Two Links (SPOTL) scheme

The final scheme that we study here is the Single-Photon Over Two Links (SPOTL) scheme, and it is another combination of the single-photon and SiSQuaRe schemes. A node is placed between Alice and Bob which tries to sequentially generate entanglement with their quantum memories by using the single-photon scheme (see Fig. 4.5). The motivation for this scheme is that, while using relatively simple components and without imposing stricter requirement on the memories than in the previous schemes, its secret-key rate would ideally scale with the fourth root of the transmissivity η.

Setup and scheme

The setup that we study is the following:

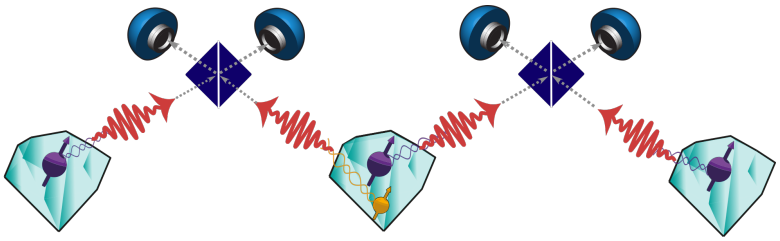


Figure 4.5: (Color on-line) Schematic overview of the setup for the SPOTL scheme. This scheme is a combination of the SiSQuaRe and single-photon scheme. Instead of sending photons directly through the fiber as in the SiSQuaRe scheme, entanglement is established between the middle node and Alice/Bob using the single-photon scheme.

SPOTL scheme

1. Alice and the repeater run the single-photon scheme until success with the tunable parameter $\theta = \theta_A$. However, only Alice performs her spin measurement immediately after each spin-photon entanglement generation attempt. This measurement is in a six-state basis.
2. The repeater swaps the state of the electron spin onto the carbon spin.
3. Bob and the repeater run the single-photon scheme until success or until the cut-off n^* is reached in which case the scheme is restarted with step 1. The tunable parameter is set here to $\theta = \theta_B$. Again, only Bob performs his spin measurement immediately after each spin-photon entanglement generation attempt and this measurement is in a six-state basis.
4. The quantum repeater performs a Bell-state measurement and communicates the result to Bob.
5. All the previous steps are repeated until sufficient data have been generated.

We note that for larger distances the optimal cut-off becomes smaller. Then, since we lose the independence of the attempts on both sides, the scaling of the secret-key rate with distance is expected to drop to $\sqrt{\eta}$, which is the same as for the single-photon scheme. However, the total distance between Alice and Bob is now split into four segments. Alice and Bob thus send photons over only one fourth of the total distance. Thus, this scheme should be able to generate key over much larger distances than the previous ones, as the dark counts will start becoming significant for larger distances only.

4.3 NV-implementation

Having proposed different quantum repeater schemes, we now move on to describe their experimental implementation based on nitrogen-vacancy centers in diamond [166]. An introduction to the NV center node can be found Sec. 1.1.3.

By applying selective optical pulses and coherent microwave rotations, we first generate spin-photon entanglement at an NV center node [158]. To generate entanglement between two distant NV electron spins, these emitted photons are then overlapped on a central beam splitter to remove their which-path information. Subsequent detection of a single photon heralds the generation of a spin-spin entangled state [158]. For all schemes based on single-photon entanglement generation, we need to employ active phase-stabilization techniques to compensate for phase shifts of the transmitted photons, which will reduce the entangled state fidelity, as introduced in Section 4.2.2. These fluctuations arise from both mechanical vibrations and temperature induced changes in optical path length, as well as phase fluctuations of the lasers used during spin-photon entanglement generation. This problem can be mitigated by using light reflected off the diamond surface to probe the phase of an effectively formed interferometer between the two NV nodes and the central beam splitter, and by feeding the acquired error signal back to a fiber stretcher that changes the relative optical path length [142].

The electron spin state can be swapped to a surrounding ^{13}C nuclear spin to free up the single optical NV interface per node for a subsequent entangling round; a weak ($\sim$ few kHz), always-on, distance-dependent magnetic hyperfine interaction between the electron and ^{13}C spin forms the basis of a dynamical decoupling based universal set of nuclear gates that allow for high fidelity control of individual nuclear spins [143, 146, 147, 10]. Crucially, the so-formed memory can retain coherence for thousands of remote entangling attempts despite stochastic electron spin reset operations, quasi static noise and microwave control infidelities during the subsequent probabilistic entanglement generation attempts [147, 167] (see Appendix A.2 for details).

In the NV node containing both the electron and carbon nuclear spin it is also possible to perform a deterministic Bell-state measurement on the two spins. Specifically, a combination of two nuclear-electron spin gates and two sequential electron spin state measurements reads out the combined nuclear-electron spin state in the Z- and X-bases, enabling us to discriminate all four Bell states [168].

For an NV center in free space, only $\sim 3\%$ of photons are emitted in the *zero-phonon-line* (ZPL) that can be used for secret-key generation. This poses a key challenge for a repeater implementation, since

this means that the probability of successfully detecting an emitted photon is low. Therefore, we consider a setup in which the NV center is embedded in an optical cavity with a high ratio of quality factor Q to mode volume V to enhance this probability via the Purcell effect in the weak coupling regime [169]. This directly translates into a lower optical excited state lifetime that is beneficial to shorten the time-window during which we detect ZPL photons after the beam splitter, reducing the impact of dark counts on the entangled state. Additionally, a cavity introduces a preferential mode into which the ZPL photons are emitted that can be picked up efficiently. This leads to a higher expected collection efficiency than the non-cavity case [149]. Enhancement of the ZPL has been successfully implemented for different cavity architectures, including photonic crystal cavities [170, 171, 172, 173, 174, 175, 176, 177], microring resonators [178], whispering gallery mode resonators [179, 180] and open, tunable cavities [181, 182, 183]. However, cavity-assisted entanglement generation has not yet been demonstrated for these systems, limited predominantly by broad optical lines of surface-proximal NV centers. Therefore, we focus on the open, tunable microcavity approach [184], since it has the potential of incorporating micron-scale diamond slabs inside the cavity, while allowing to keep high Q/V values and providing in-situ spatial and spectral tunability [185]. In these diamond slabs, an NV centre can be microns away from surfaces, potentially allowing to maintain bulk like optical and spin properties as needed for the considered repeater protocols.

4.4 Calculation of the secret-key rate

With the modeling of each of the components of the different setups in hand, the performance of each setup can be estimated. The performance of a setup is assessed in this work by its ability to generate secret key between two parties Alice and Bob. We note here that the ability of a quantum repeater to generate secret key can be measured in two different ways - in its *throughput* and its *secret-key rate*. The throughput is equal to the amount of secret key generated per unit time, while the secret-key rate equals the amount of secret key generated per *channel use*. In this chapter, we will focus on the secret-key rate only. This is due to the fact that it allows us to make concrete information-theoretical statements about our ability to generate secret key. Moreover, we note that the secret-key rate is also more universal in the sense that it can be easily converted into the throughput by multiplying it with the repetition rate of our scheme (number of attempts we can perform in a unit time).

The secret-key rate R is equal to

$$R = \frac{Y \cdot r}{N_{\text{modes}}} \ , \tag{4.1}$$

where Y and r are the yield and secret-key fraction, respectively. The yield Y is defined as the average number of raw bits generated per channel use and the secret-key fraction r is defined as the amount of secret key that can be extracted from a single raw bit (in the limit of asymptotically many rounds). Here N_{modes} is the number of optical modes needed to run the scheme. Time-bin encoding requires two modes while the single-photon scheme uses only one mode. Hence $N_{\text{modes}} = 2$ for all the schemes that use time-bin encoding in at least one of the arms of the setup. For the schemes that use only the single-photon subschemes as their building blocks we have that $N_{\text{modes}} = 1$.

In the remainder of this section, we will briefly detail how to calculate the yield and secret-key fraction, from which we can estimate the secret-key rate of each scheme.

4.4.1 Yield

The yield depends not only on the used scheme, but also on the losses in the system. We model the general emission and transmission of photons through fibers from NV centers in diamond as in Fig. 4.6. That is, with probability p_{ce} spin-photon entanglement is generated and the photon is coupled into a fiber. The photons that successfully got coupled into the fiber might not be useful for quantum information processing since they are not coherent. Thus, we filter out those photons that are not emitted at the zero-phonon line, reducing the number of photons by a further factor of p_{zpl}. Then, over the length of the fiber, a photon gets lost with probability $1-\eta_f = 1-e^{-\frac{L}{L_0}}$, where L_0 is the attenuation length and η_f is the transmissivity. After exiting the fiber the photon gets registered as a click by the detector with probability p_{det}. Finally, the photon gets accepted as a successful click if the click happens within the time-window t_{w} of the detector (see Appendix A.1 for more details).

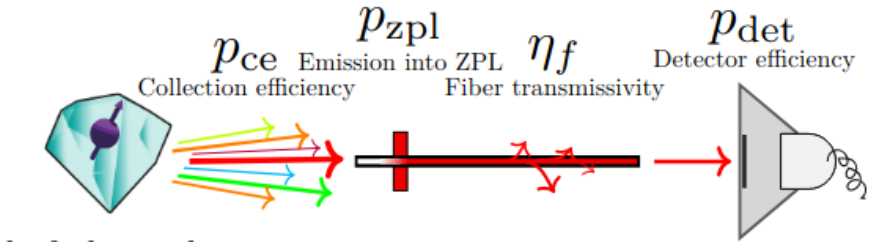


Figure 4.6: The model of photon loss proccesses occurring in our repeater setups. The parameter p_{ce} is the photon collection efficiency, which includes the probability that the photon is successfully coupled into the fiber. Only photons emitted at the zero phonon line (ZPL) can be used for quantum information processing. All non-ZPL photons are filtered out, such that a fraction p_{zpl} of the photons remains. The photons are then transmitted through a fiber with transmissivity η_f. Such successful transmissions are registered by the detector with probability p_{det}. Additionally, a significant fraction of photons can arrive in the detector outside of the detection time-window t_{w}. Such photons will effectively also get discarded. Here we describe the total efficiency of our apparatus by a single parameter, $p_{\text{app}} = p_{\text{ce}}p_{\text{zpl}}p_{\text{det}}$.

The yield can then be calculated as the reciprocal of the expected number of channel uses needed to get one single raw bit,

$$Y = \frac{1}{\mathbb{E}[N]}\ , \tag{4.2}$$

with N being the random variable that models the number of channel uses needed for generating a single raw bit.

Yield of the single-photon scheme

The yield of the single-photon scheme is relatively easy to calculate, since the single condition heralding the success of the scheme is a single click in one of the detectors in the heralding station. Therefore the yield Y is simply the probability that an individual attempt will result in a single click in one of the detectors. This probability will depend on the losses in the system, dark counts and the angle θ. A full calculation of the yield is given in Appendix A.5.

Yield of the SiSQuaRe, SPADS and SPOTL schemes

The SiSQuaRe, SPADS and SPOTL schemes require two conditions for the heralding of the successful generation of a raw bit, namely the scheme needs to succeed both on Alice's and Bob's side independently. In this case we are going to take a very conservative perspective and assume the total number of channel uses to be the sum of the required channel uses on Alice's and Bob's side of the memory repeater node

$$\mathbb{E}[N] = \mathbb{E}[N_A + N_B] \ . \tag{4.3}$$

Moreover, every time Bob reaches n^* attempts, both parties start the scheme over again. The cut-off increases the average number of channel uses, thus decreasing the yield. Denoting by p_A and p_B the probability that a single attempt of the subscheme on Alice's and Bob's side respectively succeeds, we find (see Appendix A.3 for the derivation),

$$\mathbb{E}[N_A + N_B] = \frac{1}{p_A\left(1-(1-p_B)^{n^*}\right)} + \frac{1}{p_B} \ . \tag{4.4}$$

4.4.2 Secret-key fraction

The secret-key fraction is the fraction of key that can be extracted from a single raw bit. It is a function of the average quantum bit error rates in the X-, Y- and Z-basis [186, 187] (QBER), and depends on the protocol (such as the BB84 [151] or six-state protocol [152, 153]) and classical post-processing used (such as the advantage distillation post-processing [187]).

Here we consider the entanglement-based version of the BB84 and six-state protocols. That is, Alice and Bob both perform measurements on their local qubits which share quantum correlations. We note that both the BB84 and the six-state protocol can in principle be run either in a symmetric or asymmetric way. Symmetric means that the probabilities of performing measurements in all the used bases are the same, while for asymmetric protocols they can be different. We note in the asymptotic regime, which is the regime that we consider here, it is possible to set this probability bias to approach unity and still maintain security [188]. Unfortunately, for technical reasons, within our model it is not possible to run an asymmetric six-state protocol when time-bin encoded photons are used [23].

Moreover, as we mentioned above, it is also possible to apply different types of classical post-processing of the raw key generated through the BB84 or the six-state protocol. In particular, here we consider two types of post processing: the standard one-way error correction and a more involved two-way error correction protocol called advantage distillation which can tolerate much more errors. Specifically, here we consider the advantage distillation protocol proposed in [187], as this advantage distillation protocol has high efficiency (in particular, in the scenario of no noise, the efficiency of this protocol equals unity). Hence in our model we effectively consider two protocols for generating secret key: BB84 with standard one-way error correction and six-state with advantage distillation. We refer the reader to Appendix A.7 for the mathematical expressions for the secret-key fraction for all the considered protocols.

Now we can state explicitly which QKD protocols will be considered for each scheme, which in turn depends on the type of measurements that Alice and Bob perform in that scheme. There are two physical implementations of measurements that Alice and Bob perform, depending on the scheme under consideration. That is, they either measure a quantum state of a spin or of a time-bin encoded photons. Since the fully asymmetric six-state protocol with advantage distillation has higher efficiency than both symmetric and asymmetric BB84 protocol with one-way error correction, we will use this six-state protocol for both the single-photon and SPOTL scheme. The SiSQuaRe and SPADS schemes involve direct measurement on time-bin encoded photons. Hence, for these schemes we consider the maximum of the amount of key that can be obtained using the fully asymmetric BB84 protocol and the symmetric six-state protocol with advantage distillation (which can tolerate more noise, but has three times lower efficiency than the fully asymmetric BB84 protocol).

To estimate the QBER, we model all the noisy and lossy processes that take place during the protocol run. From this, we calculate the qubit error rates and yield, from which we can retrieve the secret-key fraction. We invite the interested reader to read about the details of these calculations in Appendices A.5 and A.6. The derivation of the QBER and the yield for the SiSQuaRe scheme is performed in [23]. Moreover, in this work we introduce certain refinements to the model which we discuss in Appendix A.4. With the QBER in hand, we can calculate the resulting secret-key fraction for the considered protocols as presented in Appendix A.7.

We note here that we consider only the secret-key rate in the asymptotic limit, and that we thus do not have to deal with non-asymptotic statistics.

4.5 Assessing the performance of quantum repeater schemes

In this section we will detail four benchmarks that will be used to assess the performance of quantum repeaters. The usage of such benchmarks for repeater assessment has been done in [23, 141], and achieving a rate greater than such benchmarks can be seen as milestones towards the construction of a quantum repeater. The considered benchmarks are defined with respect to the efficiencies of processes involving photon loss when emitting photons at NV centers, transmitting them through an optical fiber and detecting them at the end of the fiber as described in Section 4.4.1 and as shown in Fig. 4.6.

Having this picture in mind, we can now proceed to present the considered benchmarks. The first three of these benchmarks are inspired by fundamental limits on the maximum achievable secret-key rate if Alice and Bob are connected by quantum channels which model quantum key distribution over optical fiber without the use of a (possible) quantum repeater.

The first of these benchmarks we consider here is also the most stringent one, the so-called *capacity of the pure-loss channel*. The capacity of the pure-loss channel is the maximum achievable secret-key rate over a channel modeling a fiber of transmissivity η_f, and is given by [129]

$$-\log_2(1-\eta_f)\ . \tag{4.5}$$

This is the maximum secret-key rate achievable, meaning that even if Alice and Bob had perfect unbounded quantum computers and memories, they could not generate secret key at a larger rate. If, by using a quantum repeater setup, a higher rate can be achieved than $-\log_2(1-\eta_f)$, we are certain our quantum repeater setup allowed us to do something that would be impossible with direct transmission. Surpassing the secret-key capacity has been widely used as a defining feature of a quantum repeater [189, 190, 191, 192, 141, 23, 127, 128, 129, 193, 194, 195]. Unfortunately, and as could be expected, surpassing the capacity is experimentally challenging. This motivates the introduction of other, easier to surpass, benchmarks. These benchmarks are still based on (upper bounds on) the secret-key capacity of quantum channels which model realistic implementations of quantum communications over fibers.

The second benchmark is built on the idea of including the losses of the apparatus into the transmissivity of the fiber. The resultant channel with all those losses included we call here *the extended channel*. The benchmark is thus equal to

$$-\log_2\left(1-\eta_f p_{\text{app}}\right) \ . \tag{4.6}$$

Here p_{app} describes all the intrinsic losses of the devices used. That is, the collection efficiency p_{ce} at the emitting diamond, the probability that the emitted photon is within the zero-phonon-line p_{zpl} (which is necessary for generating quantum correlations) and photon detection efficiency p_{det}, so that $p_{\text{app}} = p_{\text{ce}} p_{\text{zpl}} p_{\text{det}}$.

The third benchmark we consider is the so-called *thermal channel bound*, which takes into account the effects of dark counts. The secret-key capacity of the thermal channel has been studied extensively [196, 193, 195, 194, 129, 197]. We consider the following bound on the secret-key capacity of the thermal channel,

$$-\log_2\left[\left(1-\eta_f p_{\text{app}}\right)\left(\eta_f p_{\text{app}}\right)^{\overline{n}}\right] - g\left(\overline{n}\right) \ , \tag{4.7}$$

if $\overline{n} \leq \frac{\eta_f p_{\text{app}}}{1-\eta_f p_{\text{app}}}$, and otherwise zero [129]. Here $\overline{n}$ is the average number of thermal photons per channel use, and is equal to t_{w}, the time-window of the detector, times the average number of dark counts per second, see [23] for more details. The function $g(x)$ is defined as $g(x) \equiv (x+1)\log_2(x+1) - x\log_2(x)$. We note here that the time-window of the detector t_{w} is not fixed in our model, but is optimized over for every distance in order to achieve the highest possible secret-key rate. Hence in this benchmark we fix $t_{\text{w}} = 5$ ns which is the shortest duration of the time-window that we consider in our secret-key rate optimization.

Finally, the secret-key rate achieved with direct transmission using the same devices can also be seen as a benchmark. Specifically, here we mean the secret-key rate achieved when Alice uses her electron spin to generate spin-photon entanglement and sends the time-bin encoded photon to Bob. She then measures her electron spin while Bob measures the arriving photon. However, to take a conservative view, we will only use this direct transmission benchmark for the SPADS scheme. This is motivated by the fact that for both the SPADS scheme and the direction transmission scheme the experimental setups on Alice's and Bob's side are the same, ensuring that the two rates can be compared fairly. We note that similarly as in the modeled secret-key rates achievable with our proposed repeater schemes, also for this direct transmission benchmark we optimize over the time-window t_{w} for each distance.

The secret-key capacity stated in Eq. (4.5) is the main benchmark that we consider. Surpassing it establishes the considered scheme as a quantum repeater. The two expressions in Eqs. (4.6) and (4.7) and the achieved rate with direct transmission are additional benchmarks, which guide the way towards implementation of a quantum repeater. We define all the considered benchmarks for the channel with the same fiber attenuation length L_0 as the channel used for the corresponding achievable secret-key rate.

4.6 Numerical results

We now have a full model of the rate of the presented quantum repeater protocols as a function of the underlying experimental parameters. In this section we will firstly state all the parameters required by our model and then present the results and conclusions drawn from the numerical implementation of this model. In particular, in Section 4.6.1 we will first provide a deeper insight into the benefits of using the six-state protocol and advantage distillation in specific schemes. In Section 4.6.2 we determine the optimal positioning of the repeater nodes for our schemes and investigate the dependence of the secret-key rate achievable with those schemes on the photon emission angle θ and the cutoff n^* for the appropriate schemes. In Section 4.6.3 we then use the insights acquired in the previous section to compare the achievable secret-key rates for all the proposed repeater schemes with the secret-key capacity and other proposed benchmarks. In particular, we show that the single-photon scheme significantly outperforms the secret-key capacity and hence can be used to demonstrate a quantum repeater. Finally, in Section 4.6.4 we determine the duration of the experiment that would allow us to demonstrate such a quantum repeater with the single-photon scheme.

The parameters that we will use are either parameters that have been achieved in an experiment, or correspond to expected parameters when the NV center is embedded in an optical Fabry-Perot microcavity. The parameters we will use are listed below:

- a_0 (dephasing of ^{13}C due to interaction) = $\frac{1}{2000}$ per attempt [147, 167]
- a_1 (dephasing of ^{13}C with time) = $\frac{1}{3}$ per second [9]
- b_0 (depolarizing of ^{13}C due to interaction) = $\frac{1}{5000}$ per attempt [147]
- b_1 (depolarizing of ^{13}C with time) = $\frac{1}{3}$ per second [9]
- t_{prep} (memory-photon entanglement preparation time) = 6 μs [156]
- F_m (depolarizing parameter for the measurement of the electron spin) = 0.95 [142]
- F_g (depolarizing parameter for two qubit gates in quantum memories) = 0.98 [10]
- F_{prep} (dephasing parameter for the memory-photon state preparation) = 0.99 [156]
- p_{ce} (collection efficiency) = 0.49 [156, 149]
- p_{zpl} (emission into the zero phonon line) = 0.46 [183]
- p_{det} (detector efficiency) = 0.8 [156]
- Dark count rate = 10 per second [156]
- τ (characteristic time of the NV emission) = 6.48 ns [183, 198]
- $t_{\text{w}}^{\text{offset}}$ (detection window offset) = 1.28 ns [156]
- L_0 (attenuation length) = 0.542 km [156]
- n_{ri} (refractive index of the fiber) = 1.44 [199]
- $\Delta\phi$ (optical phase uncertainty of the spin-spin entangled state) = 14.3° [142]

To be more specific, the photon collection efficiency p_{ce} and the probability of emitting into the zero phonon line p_{zpl} are the two crucial parameters relying on the implementation of the optical cavity. The quoted value of p_{ce} has not been experimentally demonstrated yet, while the value of p_{zpl} has not been demonstrated in the context of quantum communication. All the other independent parameters in the above list that are not related to the setup with a cavity, have been demonstrated in experiments relevant for remote entanglement generation. The parameters that have not been discussed in the main text are discussed in the appendix.

4.6.1 Comparing BB84 and six-state advantage distillation protocols

We first investigate here when the BB84 or six-state advantage distillation protocol performs better. It was shown in [23] that in the SiSQuaRe scheme there is a trade-off - for the low noise regime (small distances) the fully asymmetric BB84 protocol is preferable, while in the high noise regime (large distances) the problem of noise can be overcome by using a six-state protocol supplemented with advantage distillation. This technique allows us to increase the secret-key fraction at the expense of reducing the yield by a factor of three, since a six-state protocol in which Alice and Bob perform measurements on photonic qubits does not allow for the (fully) asymmetric protocol within our model. Numerically, we find that for the SPADS and SPOTL scheme advantage distillation is *necessary* to generate non-zero secret-key at any distance. This is due to the fact that there is a significant amount of noise in these schemes. Thus, for the SPADS (SPOTL) scheme the (a)symmetric six-state protocol with advantage distillation is optimal.

To provide more insight into the performance of those different QKD schemes for different parameter regimes, we plot the achievable secret-key fraction for the SPADS and SPOTL schemes as a function of the depolarizing parameter due to imperfect electron spin measurement F_m in Figure 4.7 (see Appendix A.2 for the discussion of the corresponding noise model). Noise due to imperfect measurements is one of the significant noise sources in our setup, since the SPADS scheme involves three and the SPOTL scheme four single-qubit measurements on the memory qubits. The data have been plotted for a fixed distance of $12.5L_0$, where $L_0 = 0.542$ km is the attenuation length of the fiber. Moreover, since on this plot we aim at maximizing only the secret-key fraction over the tunable parameters, we set the cutoff n^* to one and the detection time-window t_{w} to 5 ns (the smallest detection time-window we use) for both schemes. Furthermore, within the single-photon subscheme the heralding station is always placed exactly in the middle between the two memory nodes. We also consider the positioning of the memory repeater node to be two-thirds away from Alice for the SPADS scheme and in the middle for the SPOTL scheme as discussed in the next section. For the SPOTL scheme we also assume $\theta_A = \theta_B$ which we will justify in the next section.

We see that for the current experimental value of $F_m = 0.95$ both schemes can generate key only if the advantage distillation post-processing is used. As F_m increases, we observe that for the SPADS scheme firstly the six-state protocol without advantage distillation and then the BB84 protocol start generating key. For the SPOTL scheme the value of F_m at which the six-state protocol without advantage distillation starts generating key is much larger than the corresponding value of F_m for any of the studied protocols for the SPADS scheme. This is because the SPOTL scheme involves more noisy processes than the SPADS scheme. This also provides an approximate quantification of the benefit of using advantage

distillation. Specifically, looking at the SPOTL scheme, it can be observed that while at the current experimental value of $F_m = 0.95$ advantage distillation allows for generating key, at a higher value of the depolarizing parameter $F_m = 0.97$, still no key can be generated with standard one-way post-processing. Moreover, we see that utilizing advantage distillation for the SPADS scheme allows for the generation of key, even with very noisy measurements when $F_m = 0.91$. We also observe two distinct scalings of the secret-key fraction with F_m in the regime where non-zero amount of key is generated. These two scalings depend on whether we use a symmetric or asymmetric protocol. Specifically, for the SPADS scheme the symmetric six-state protocol is used. Therefore the corresponding two curves have a slope that is approximately three times smaller than the other three curves corresponding to the protocols that run in the fully asymmetric mode.

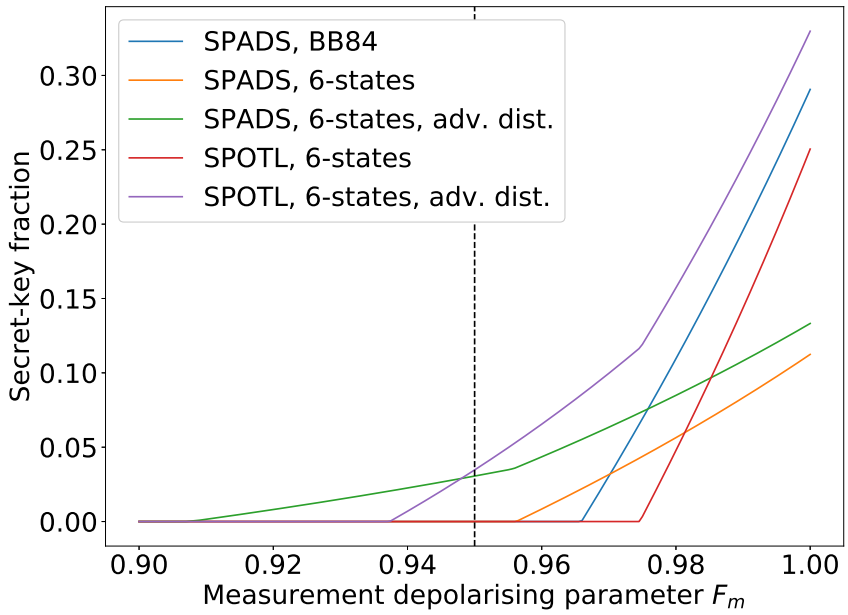


Figure 4.7: (Color on-line) Secret-key fraction as a function of the depolarizing parameter due to noisy measurement F_m for the total distance of $12.5L_0$. We see that for the current experimental value of $F_m = 0.95$ (marked with a dashed black vertical line) both schemes can generate key only if the advantage distillation post-processing is used. As F_m increases the protocols that do not utilize advantage distillation also start generating key. We also see that the curves can be divided into two groups in terms of their slope in the regime where they generate non-zero amount of key. Those two groups correspond to the scenarios where a fully asymmetric (bigger slope) or a symmetric (smaller slope) protocol is used. For all the plotted protocols the cutoff n^* is set to one and $t_w = 5$ ns (the smallest detection time-window we use) to maximize the secret-key fraction. Moreover, for each value of F_m we optimize the secret-key fraction over the angle θ. For the SPOTL scheme we assume $\theta_A = \theta_B$. For the SPADS scheme we position the repeater node 2/3 away of the total distance from Alice and in the middle between Alice and Bob for the SPOTL scheme.

This page is left blank to help with the reading.

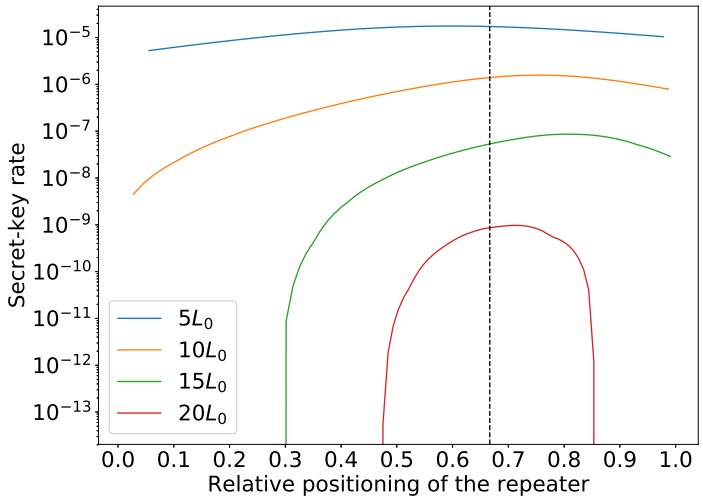


Figure 4.8: (Color on-line) Secret-key rate as a function of the relative positioning of the repeater for few different total distances for the SPADS scheme. The total distances are expressed in terms of the fiber attenuation length $L_0 = 0.542$ km. We see that positioning the repeater two-thirds of the distance away from Alice (marked by the vertical black dashed line) is a good positioning for all the distances. For each total distance considered and each positioning the secret-key rate is optimized over the cutoff n^*, the angle θ and the time-window of the detector t_{w}.

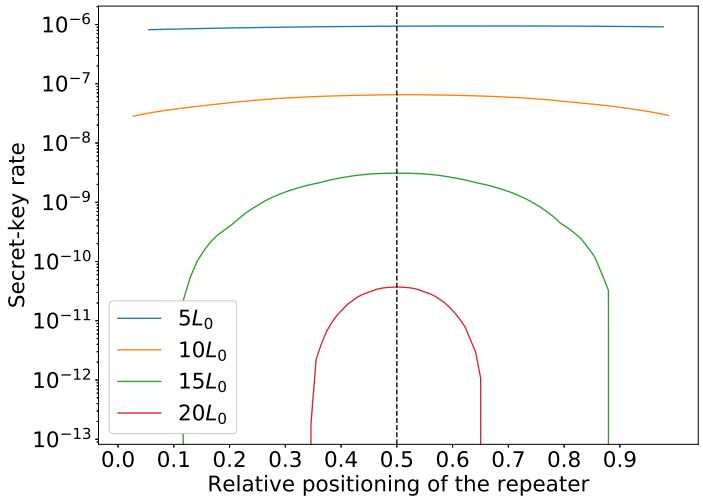


Figure 4.9: (Color on-line) Secret-key rate as a function of the relative positioning of the repeater for few different total distances for the SPOTL scheme. The total distances are expressed in terms of the fiber attenuation length $L_0 = 0.542$ km. We see that positioning the repeater in the middle between Alice and Bob (marked by the vertical black dashed line) is a good positioning for all the distances. For each total distance considered and each positioning the secret-key rate is optimized over the cutoff n^*, the angles θ_A and θ_B and the time-window of the detector t_{w}.

4.6.2 Optimal settings

We see that the above described repeater schemes include several tunable parameters. These parameters are the cut-off n^* for Bob's number of attempts until restart, the angle θ in the single-photon scheme and the positioning of the repeater. These parameters can be optimized to maximize the secret-key rate. Here we will approach this optimization in a consistent way - we gradually restrict the parameter space by making specific observations based on numerical evidence.

The first claim that we will make is in relation to the *optimal positioning of the repeater*. In [23] we have conjectured that for the SiSQuaRe scheme the middle positioning of the repeater is optimal. For the single-photon scheme we want the probability of transmitting the photons from each of the two nodes to the beam splitter heralding station to be equal. This effectively sets the target state between the electron spins to be the maximally entangled state. Hence, if we restrict ourselves to the case where the emission angles θ of both Alice and Bob are the same, then it is natural to position the heralding station symmetrically in the middle between them. Hence, the only non-obvious optimal positioning is for the SPADS and SPOTL scheme.

For the SPADS scheme, positioning the repeater at two-thirds of the relative distance away from Alice could intuitively be expected to be optimal. This is due to the fact that the single-photon scheme runs on two segments: Alice-beam splitter, beam splitter-repeater, while the one half of the SiSQuaRe scheme runs only over a single segment between repeater and Bob. By segment we mean here a distance over which we need to be able to independently transmit a photon. In Fig. 4.8 we show the secret-key rate as a function of the relative positioning of the repeater for a set of different total distances. We see there that despite the fact that positioning the repeater at two-thirds is not always optimal, it is a good enough positioning for all distances for our purposes. For each data point on the plot we independently optimize over the cut-off n^*, the angle θ of the single-photon subscheme and the duration of the detector time-window t_{w}.

The SPOTL scheme has the same symmetry as the SiSQuaRe scheme, in the sense that the part of the scheme performed on Alice's side is exactly the same as on Bob's side. This symmetry is only broken by the sequential nature of the scheme. Since we have already observed that the middle positioning is optimal for the SiSQuaRe scheme, we expect to see the same behavior for the SPOTL scheme. Indeed, we confirm this expectation numerically in Fig. 4.9. Here for each data point we independently optimize over the cut-off n^*, the angle θ_A (θ_B) of the single-photon subscheme on Alice's (Bob's) side and the duration of the detection time-window.

To conclude, we will always place the heralding station within the single-photon (sub)protocol exactly in the middle between the two corresponding memory nodes. Moreover, we will also always place the memory repeater node in the middle for the SPOTL scheme and two-thirds of the distance away from Alice for the SPADS scheme.

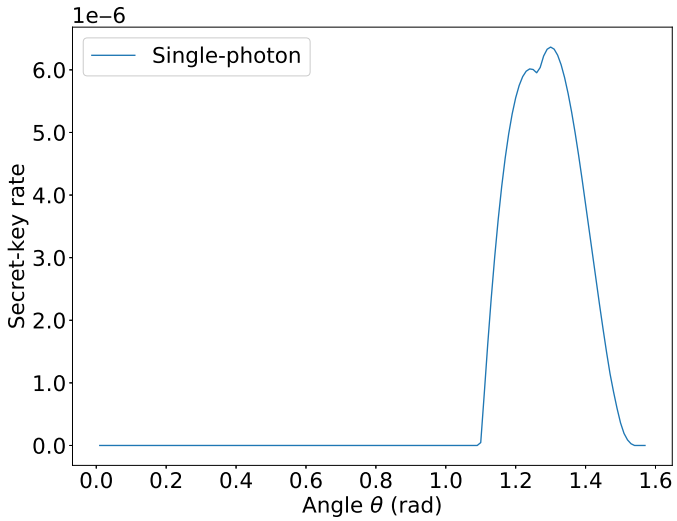


Figure 4.10: (Color online) Secret-key rate as a function of the θ angle for the single-photon scheme for the total distance of $12.5L_0$, where $L_0 = 0.542$ km. We see that there is a relatively large range of angles for which non-zero amount of key can be generated. For each value of θ the secret-key rate is optimized over the time-window t_{w}. The kink on the plot is a consequence of the fact that the six-state protocol with advantage distillation involves optimization over of two subprotocols.

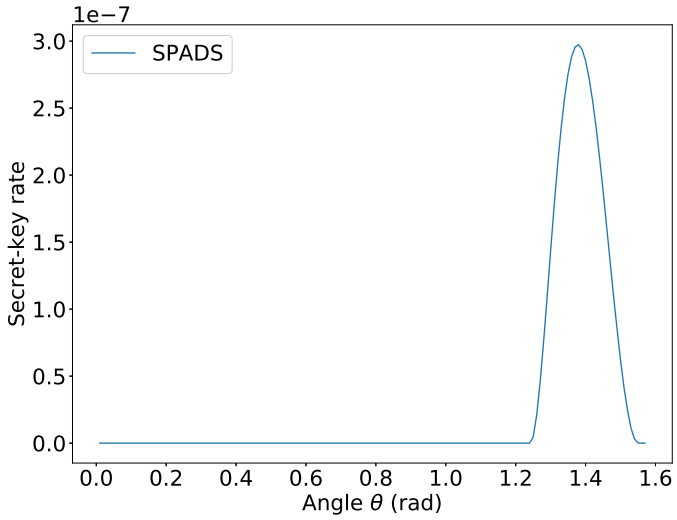


Figure 4.11: (Color on-line) Secret-key rate as a function of the θ angle for the SPADS scheme for the total distance of $12.5L_0$, where $L_0 = 0.542$ km. We see that due to more noisy processes the range of θ that allows us to generate key is much more restricted than for the single-photon scheme. For each value of θ the secret-key rate is optimized over the cutoff n^* and the time-window t_{w}.

Having established the optimal positioning of the repeater, we look into the relation between θ_A and θ_B for the SPOTL scheme. We observe that the relative error resulting from optimizing the secret-key rate over a single angle $\theta_A = \theta_B$ rather than two independent ones is smaller than 1% for all distances. Hence from now on we will restrict ourselves to optimizing only over one angle θ for the SPOTL scheme.

Having resolved the issues of the optimal positioning of the repeater for all schemes and reducing the number of angles to optimize over for the SPOTL scheme to one, we now investigate how our secret-key rate depends on the remaining parameters. These parameters are the angle θ, the cut-off n^* and the duration of the detection time-window t_{w}. The optimal time-window follows a simple behavior for all schemes: for short distances the probability of getting a dark count p_d is negligible compared to the probability of detecting the signal photon. Hence for those distances we can use a time-window of 30 ns to make sure that almost all the emitted photons which are not polluted by the photons from the optical excitation pulse arrive inside the detection time-window. We always need to sacrifice the photons arriving within the time $t_{\mathrm{w}}^{\mathrm{offset}}$ after the optical pulse has been applied to filter out the photons from that pulse, see Appendix A.1 for details. Then, for larger distances where p_d starts to become comparable with the probability of detecting the signal photon, the duration of the time-window is gradually reduced. This reduces the effect of dark counts at the expense of having more and more photons arriving outside of the time-window. See Appendix A.1 for the modeling of the losses resulting from photons arriving outside of the time-window.

The dependence of the secret-key rate on the angle θ, the tunable parameter that Alice and Bob choose in their starting state $|\psi\rangle = \sin\theta\,|{\downarrow}\rangle\,|0\rangle + \cos\theta\,|{\uparrow}\rangle\,|1\rangle$ in the single-photon scheme, is more complex. We observe that the optimal value of θ is closer to $\frac{\pi}{2}$ for schemes that involve more noisy processes. Informally, this means that Alice and Bob send 'less' photons towards the beam splitter, to overcome the noise coming from events in which both nodes emit a photon. At $\frac{\pi}{2}$ however, no photons are emitted and the rate drops down to zero. We illustrate this in Figs. 4.10, 4.11, and 4.12. We see that for the SPADS and SPOTL scheme, there is only a restricted regime of the angle θ for which one can generate non-zero amount of key. In particular, the SPOTL scheme requires a larger number of noisy operations, and therefore cannot tolerate much noise arising from the effect of photon loss in the single-photon subscheme. This means that there is only a small range of θ that allows for production of secret key. The single-photon scheme involves much less operations and can tolerate more noise, and so lower values of the parameter θ still allow for the generation of key.

We also investigate the dependence of the rate on the cut-off. Both the SPADS and SPOTL scheme require a lower cut-off than the SiSQuaRe scheme, see Fig. 4.13 and 4.14. This is caused by the fact that each of them involves more noisy operations, and hence less noise tolerance is possible.

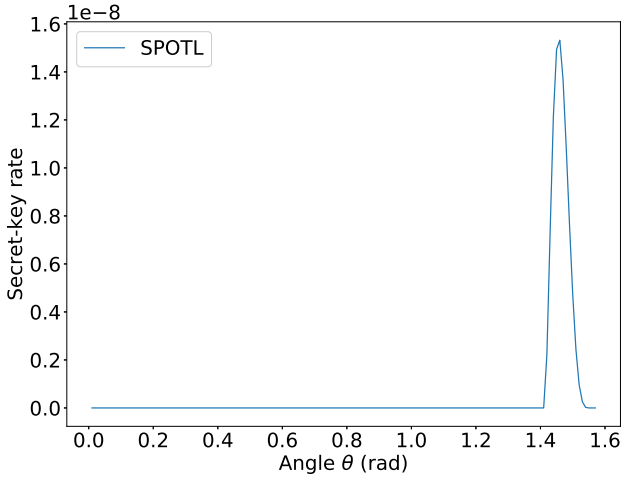


Figure 4.12: (Color on-line) Secret-key rate as a function of the angle $\theta = \theta_A = \theta_B$ for the SPOTL scheme for the total distance of $12.5L_0$, where $L_0 = 0.542$ km. We see that, due to the increased amount of noisy processes, this scheme requires θ to be in a much narrower regime than for the single-photon and SPADS schemes, as can be seen by comparing the plot with the plots in FIG. 4.10 and in FIG. 4.11. This corresponds to the overwhelming dominance of the dark state of the spin (no emission of the photon) in order to avoid any extra noise coming from the photon loss. For each value of θ the secret-key rate is optimized over the cutoff n^* and the time-window t_{w}.

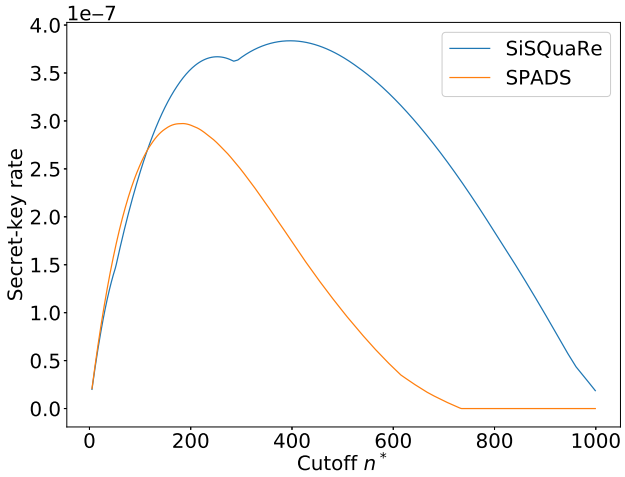


Figure 4.13: (Color on-line) Secret-key rate as a function of the cut-off for the SiSQuaRe and SPADS scheme for the total distance of $12.5L_0$, where $L_0 = 0.542$ km. We see that the SPADS scheme requires lower cut-off than the SiSQuaRe scheme because it involves more noisy operations. For each value of the cutoff n^* we optimize the secret-key rate over the time-window t_{w} and for the SPADS scheme also over the θ angle. The kink for the SiSQuaRe scheme arises because of the optimization over the fully asymmetric one-way BB84 protocol and symmetric six-state protocol with advantage distillation, which itself involves optimization over two subprotocols.

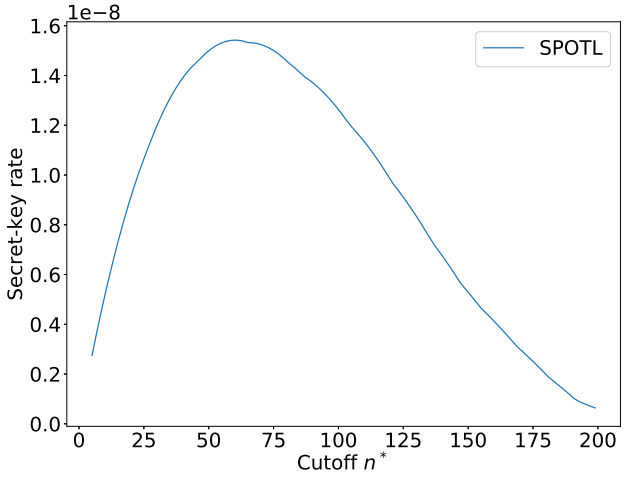


Figure 4.14: (Color on-line) Secret-key rate as a function of the cut-off for the SPOTL scheme for the total distance of $12.5L_0$, where $L_0 = 0.542$ km. We see that due to the large number of noisy operations, this scheme requires a low cut-off in order to be able to generate key. For each value of the cutoff n^* we optimize the secret-key rate over the time-window t_{w} and the θ angle.

4.6.3 Achieved secret-key rates of the quantum repeater proposals

Now we are ready to present the main results, the secret-key rate for all the considered schemes as a function of the total distance when optimized over θ, the cut-off n^* and the duration of the time-window t_{w}. We compare the rates to the benchmarks from Section 4.5.

In Fig. 4.15 we plot the rate of all four of the quantum repeater schemes as a function of the distance between Alice and Bob. We recall that L_0 is the attenuation length of the fiber, such that there is a probability $\eta(L) = \exp(L/L_0)$ that a photon is lost after distance L. We observe that already for realistic near-term parameters, the single-photon scheme can outperform the secret-key capacity of the pure-loss channel by a factor of seven.

We have also investigated what improvements would need to be done in order for the SPADS and SPOTL schemes to also overcome the secret-key capacity. An example scenario in which the SPADS scheme outperforms this repeaterless bound includes better phase stabilization such that $\Delta\phi = 5°$ and reduction of the decoherence effects in the carbon spin during subsequent entanglement generation attempts such that $a_0 = 1/8000$ and $b_0 = 1/20000$. Further improvement of these effective coherence times to $a_0 = 1/20000$ and $b_0 = 1/50000$ allows the SPOTL scheme to also overcome the secret-key capacity. We note that maintaining coherence of the carbon-spin memory qubit for such large number of subsequent remote entanglement generation attempts is expected to be possible using the method of decoherence-protected subspaces [147, 167].

As mentioned before, the SPADS scheme can be naturally compared against the benchmark of the direct transmission using NV as a source. The results are depicted in Fig. 4.16. We see that the SPADS scheme easily overcomes the NV-based direct transmission and the thermal benchmark for larger distances for which these benchmarks drop to zero.

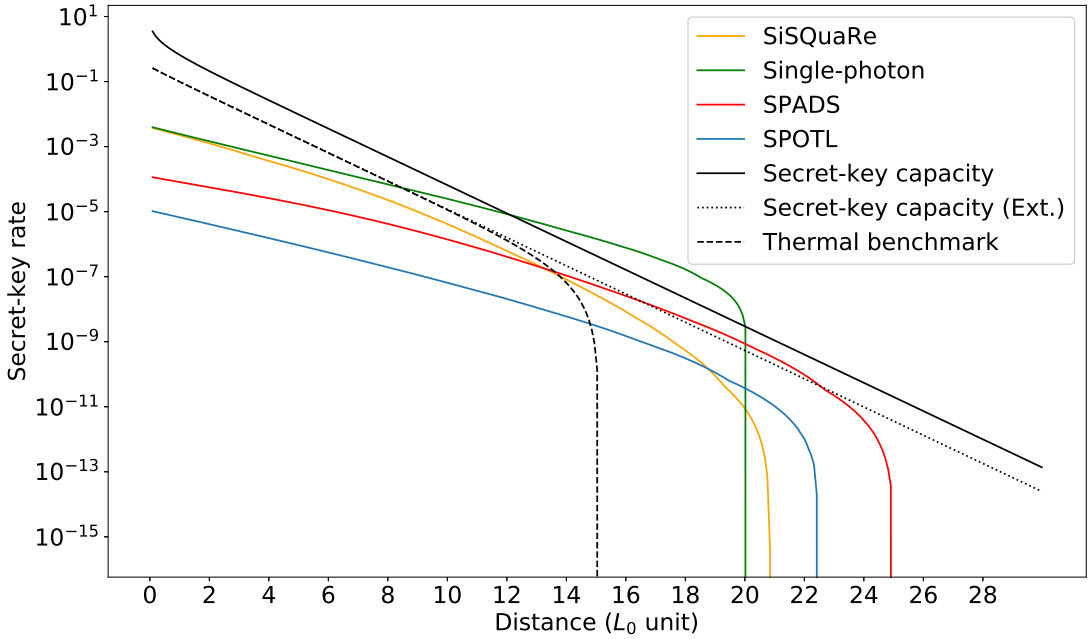


Figure 4.15: (Color on-line) Rate of all studied quantum repeater schemes as a function of the distance between Alice and Bob, expressed in the units of $L_0 = 0.542$ km. We also plot the different benchmarks from Section 4.5. We see that the single-photon scheme outperforms the secret-key capacity. For the achievable rates the secret-key rate is optimized over the cutoff n^*, the angle θ and the time-window t_w independently for each distance.

In Fig. 4.15 we observe that for the SPOTL scheme, the total distance over which key can be generated is significantly smaller than for the SPADS scheme. This is despite the fact that the full distance is divided into four segments. The rather weak performance of this scheme is due to the fact that it involves a larger number of noisy operations. As a result, the scheme can tolerate little noise from the single-photon subscheme, requiring the angle θ to be close to $\frac{\pi}{2}$ as can be seen in Fig. 4.12. As a result, the probability of photon emission becomes greatly diminished and so the distance after which dark counts start becoming significant is much smaller than for the SPADS scheme. To overcome this problem one would need to reduce the amount of noise in the system. One of the main sources of noise is the imperfect single-qubit measurement. Hence we illustrate the achievable rates for the scenario with the boosted measurement depolarizing parameter $F_m = 0.98$ in Fig. 4.17. Additionally, in this plot we also consider the application of probabilistic frequency conversion to the telecom wavelength at which $L_0 = 22$ km. Frequency conversion has already been achieved experimentally in the single-photon regime with success probability of 30% [200]. This is also the success probability that we consider here. The corresponding benchmarks have also been plotted for the new channel with $L_0 = 22$ km. We see in Fig. 4.17 that with the improved measurement and using frequency conversion, the SPOTL scheme allows now to generate secret key over more than 550 km. We also see that under those conditions the single-photon scheme can also overcome the secret-key capacity of the telecom channel.

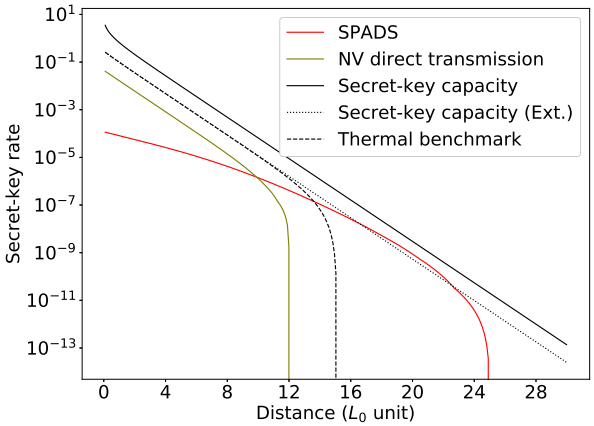


Figure 4.16: (Color on-line) Comparison of the SPADS scheme with the rate achievable using the direct transmission, with NV being the photon source. The secret-key rates for those schemes are plotted as a function of the distance between Alice and Bob, expressed in the units of $L_0 = 0.542$ km. We also plot the different benchmarks. We see that the SPADS scheme easily overcomes the direct transmission and the thermal benchmark (see Section 4.5). For the secret-key rate achievable with the SPADS scheme we perform optimization over the cutoff n^*, the angle θ and the time-window t_{w} independently for each distance. Similarly, we also optimize the secret-key rate achievable with direct transmission over the time-window t_{w}.

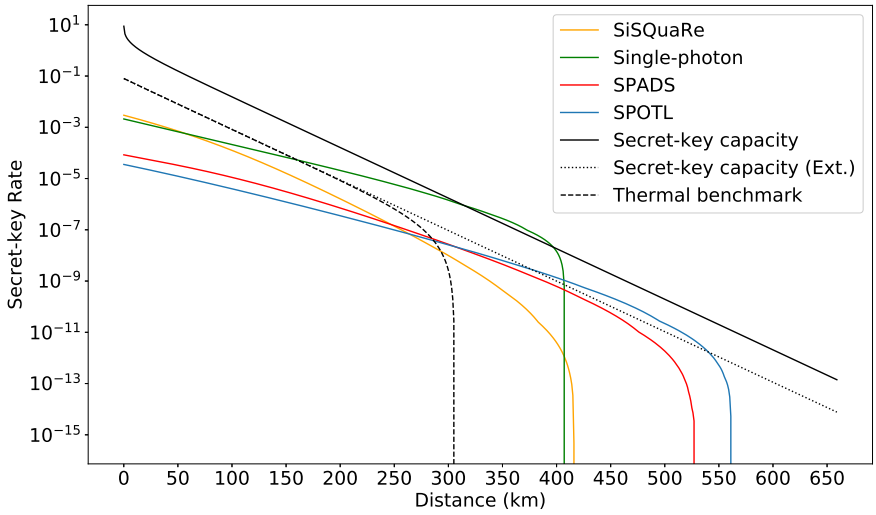


Figure 4.17: (Color on-line) Secret-key rate as a function of distance in units of km for transmission at telecom channel with $L_0 = 22$ km, along with the benchmarks from Section 4.5. We consider an improved measurement depolarizing parameter of $F_m = 0.98$. The frequency conversion efficiency is assumed to be 0.3. We observe that the SPOTL scheme allows for the generation of secret-key over a distance of more than 550 km. For the achievable rates the secret-key rate is optimized over the cutoff n^*, the angle θ and the time-window t_{w} independently for each distance.

4.6.4 Runtime of the experiment

While the theoretical capability of an experimental setup to surpass the secret-key capacity is a necessary requirement to claim a working quantum repeater, it does not necessarily mean that this can be experimentally verified in practice. Indeed, if a quantum repeater proposal only surpasses the secret-key capacity by a narrow margin at a large distance, the running time of an experiment could be too long for practical purposes. In this section, we will discuss an experiment which can validate a quantum repeater setup and calculate the running time of such an experiment, where we demonstrate that the single-photon scheme could be validated to be a quantum repeater within twelve hours.

A straightforward way of validating a quantum repeater would consist of first generating secret-key, calculating the achieved (finite-size) secret-key rate and then comparing the rate with the secret-key capacity. However, this requires a large number of raw bits to be generated, partially due to the loose bounds on finite-size secret-key generation. What we propose here is an experiment where the QBER and yield are separately estimated to lie within a certain confidence interval. Then, if with the (worst-case) values of the yield and the QBER the corresponding asymptotic secret-key rate still confidently beats the benchmarks, one could claim that, in the asymptotic regime, the setup would qualify as a quantum repeater.

As we show in Appendix A.8, it is possible to run the single-photon scheme over a distance of $17L_0 \approx 9.2$ km for approximately twelve hours to find with high confidence ($\geq 1 - 1.5 \cdot 10^{-4}$) that the scheme beats the capacity (see Eq. (4.5)) at that distance by a factor of at least three.

4.7 Conclusions

We analyzed four experimentally relevant quantum repeater schemes on their ability to generate secret key. More specifically, the schemes were assessed by contrasting their achievable secret-key rate with the secret-key capacity of the channel corresponding to direct transmission. The secret-key rates have been estimated using near-term experimental parameters for the NV center platform. The majority of these parameters have already been demonstrated across multiple experiments. A remaining challenging element of our proposed schemes is the implementation of optical cavities. These cavities would enable the enhancement of both the photon emission probability into the zero-phonon line and the photon collection efficiency to the desired level.

With these near-term experimental parameters, our assessment shows the viability of one of the schemes, the single-photon scheme, for the first experimental demonstration of a quantum repeater. In fact, the single-photon scheme achieves a secret-key rate more than seven times greater than the secret-key capacity. We also estimated the duration of an experiment to conclude that a rate larger than the secret-key capacity is achievable. The duration of the experiment would be approximately twelve hours.

Finally, we show that a scheme based on concatenating the single-photon scheme twice (i.e. the SPOTL scheme), has the capability to generate secret-key at large distances. However, this requires converting the frequency of the emitted photons to the telecom wavelength and modestly improving the fidelity at which measurements can be performed.

This simulation work allowed us to understand in depth the challenges around long-distance bipartite communications and quantum repeaters. We saw that there is a distance where a NV-based repeater protocol can generate key between two nodes at a higher rate than using direct transmission. However, this rate, that we achieved using state of the art parameters for our nodes, is still very small and not suited for practical use. The experimental causes of this low rate are two-folds: the generation of entanglement between two neighbouring node is too slow and the swapping of the entanglement is too noisy. The former is mostly due to the low probability of emitting a photon using the electron spin of the NV-center and the latter to the noise in the memory caused by the coupling between the two NV qubits.

While yielding interesting data about repeater protocols with NV centers, this study hints the impracticality of quantum repeaters with today's abilities. Even at low distances, the noise added by the repeating operations lowers the achieved secret key rate. For distances over 50km, there are very few use cases in which the achieved rate could prove useful. In the rest of this thesis we will focus on repeaterless quantum communications, first by looking at short-distance metropolitan networks and then by analyzing alternatives to fiber-based communications at long distance.

Chapter 5

Feasibility of metropolitan Quantum Networks

In the rest of this thesis, we take a more concrete step towards the realization of a realistic architecture for the Quantum Internet. As explained in the previous chapter, one of the main obstacles towards building a full scale Quantum Internet is long distance quantum communication. Here, we wish to show that a number of quantum network applications are in fact accessible at a metropolitan level even with near-term technology. Our goal is to contribute to the identification of network topologies and system architectures that can enhance today's communications with quantum-enabled functionalities in a realistic and practical way, while more advanced technologies gradually become available and upgrade the network. We take inspiration from the methods used in the previous chapter to create a loss and noise model for photonic quantum networking, that we embed into a network simulator. We will tackle the issue of long-distance communication with alternatives to fiber in the next chapter.

Contribution and outline: Here, we create a model for metropolitan photonic quantum networks, that we call the Quantum City, which we detail in Sec. 5.1. Close discussions with experimentalists allowed us to create a realistic model of all the processes that happen during a network protocol, from creation, sending and detection of a qubit. We also show this modeling in this section. In Sec 5.2, we then assess today's and near future networking capabilities by performing simulation based on a library of function using Netsquid, a network simulator developed at QuTech in Delft. We simulate our Quantum City architecture on a realistic instance in Paris and analyze the simulations of bipartite and multipartite applications. We hope that this study will help future developments by highlighting the important hardware parameters limiting quantum Internet development.

Article link: The manuscript will be submitted within the next few weeks.

5.1 The Quantum City

We propose an architecture for a metropolitan scale quantum network that minimizes end user hardware, that we call the Quantum City. It should have all the properties desired from a network architecture in development namely support distributed quantum applications, enhance today's networking ability, allow for growth and adaptability to tomorrow's applications, support hardware heterogeneity, be easy to manage, be resilient to failure and malicious actors and work as soon as possible (see Sec. 1.3.1 for more details).

5.1.1 Architecture description

In this section we describe the Quantum City, a realistic architecture for photonic quantum networks. In its basic form, it has a star topology with a central node that we call Qonnector linked to a number of users that we call Qlients through optical fibers (see Fig. 5.1). This allows for centralized routing procedures and asymmetric distribution of hardware between a powerful Qonnector and very limited Qlients. This corresponds well to the expected intermediate-term development of quantum networks, where some nodes with advanced quantum resources will be providing quantum access and functionalities to a number of users with very limited quantum capabilities. Below we describe precisely the abilities of a Qonnector and a Qlient node in our model.

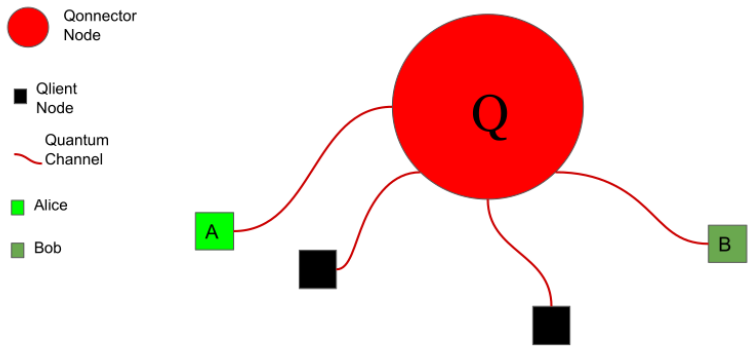


Figure 5.1: The Quantum City topology. It is a photonic star quantum network with a special node in the middle, the Qonnector, that has advanced quantum capabilities. Each end node (Qlient) has very limited quantum capabilities and is connected to the Qonnector through an optical fiber. The Quantum City allows for Qlients to perform quantum protocols via the Qonnector.

Qonnector nodes provide the core quantum functionalities of our model. They are an abstraction of quantum servers providing quantum services to end users. The capabilities of a Qonnector may vary and evolve in time, but in principle they are nodes that can create and share multipartite photonic quantum states and are connected both classically and quantumly to a certain number of users from whom they can receive photons and perform measurements on them. Using state-of-the-art photonic technology, we can already assume that a Qonnector has a number of capabilities: to create and manipulate any one-qubit state as well as multiparty entangled states such as Bell pairs and GHZ states up to a certain number of qubits; to receive and measure any photonic state and to perform probabilistic Bell state measurements on two photons arriving simultaneously; to route photonic states arriving from one Qlient to another Qlient.

A Qonnector will also use classical computing power and classical Internet. In particular, a Qonnector holds a list of each Qlient's identification and port to use to communicate with each of them. It also has empty classical memory slots reserved for each connected Qlient to perform classical post and pre-processing in protocols. This centralizes network information in one node, facilitating routing of quantum information and addition of new Qlients to the network. In a metropolitan area, a Qonnector able to perform those specific tasks provides the resource for the creation of a quantum network of tens or hundreds of users. A Qonnector thus represents a network provider for an area.

As mentioned before, one can imagine even more powerful Qonnectors, for example a node equipped with quantum memories to enable efficient, on-demand operations, or with a quantum processor to which a Qlient can delegate securely a computation. Distant Qonnectors may also be linked with quantum repeater or satellite links, forming a backbone network with entangled central nodes. Our architecture is agile enough to handle such upgrades in the quantum capabilities of the Qonnector nodes, while making it possible for the quantum network to support a number of different functionalities already with a simple state-of-the-art photonic node as a Qonnector and Qlients with limited and realistic quantum capabilities.

Qlient nodes represent the end users connecting to the quantum network. They abstract private users that hold photonic quantum communication devices expected to be commercially available in the near future. They are classically connected to the rest of the network through the classical Internet and have usual classical computing power. We assume that they have very limited quantum hardware capabilities namely they can manipulate one qubit at a time. More precisely they can generate, receive and measure any one-qubit photonic state (in fact, it may be sufficient to have the ability to either generate or receive and measure such states). In a more advanced version, Qlients also have the capability to store quantum states for a short period of time. Industrial-grade devices offering these capabilities are already available today or will become in the near future, and can be expected to become more suitable for wider use in the following years, thanks to advances for instance in photonic integration [201].

As we will show in the rest of this work, even in the most restricting memory-less setup, Qlients have access to various quantum-enhanced functionalities, including performing Quantum Key Distribution, conference agreement, anonymous transmission, E-voting and others. The architecture is easily scalable as adding a Qlient only amounts to connecting it to the Qonnector through an optical fiber. Moreover, through entanglement with the Qonnector, Qlients have the power to securely and privately perform remote computation on a more powerful device. A Qonnector node that possesses or is connected to a quantum computer would let any Qlient to securely enjoy universal quantum computation, thanks to blind and verifiable delegated computing protocols that only requires a series of one-qubit states provided by the Qlient [78].

Given the fact that it seems highly unrealistic that all nodes of future quantum networks will be able to perform universal quantum computation or even to store qubits in quantum memories at home, such more centralised networks provide a realizable way forward for quantum communications.

Last, a Quantum City is compatible with the longer-term vision of a Quantum Internet, where nodes use quantum memories to share entanglement between them in order to transmit quantum information via teleportation. Qonnector nodes can play such a role, creating a backbone quantum

network that creates entanglement between the central nodes of different metropolitan networks, via repeater or satellite links. Nevertheless, one need not wait for such capabilities to become deployable before developing functional metropolitan quantum networks in the coming years.

5.1.2 Modelling Quantum Processes

Let us now go into more detail in the operations that the nodes of our network architecture can perform, to include in particular losses and errors that are inherent in any realistic quantum operation. As in the previous chapter, we model losses and errors through depolarizing and dephasing channels that act on the state ρ on which the operation is applied:

$$\begin{aligned} \mathcal{D}^{\lambda_1}_{\text{depol}}(\rho) &= \lambda_1 \rho + (1-\lambda_1)\frac{\mathbb{I}}{d} \ , \\ \mathcal{D}^{\lambda_2}_{\text{dephase}}(\rho) &= \lambda_2 \rho + (1-\lambda_2) Z\rho Z \ , \end{aligned} \tag{5.1}$$

where λ_1 represents losses and λ_2 represents noise. Every time a specific operation is applied to a qubit, these channels describe the applied operation with its corresponding parameters. In other words, λ_1 corresponds to a loss probability and λ_2 to an error probability. In this work we focus on photonic quantum communication, thus we suppose qubits cannot be stored and we don't consider decoherence effects. More precisely we will consider the following sources of losses and errors:

- The creation of any one-qubit state $|\psi\rangle = \cos\theta\,|0\rangle + \sin\theta\,|1\rangle$ is attempted at a rate f_{qubit} and succeeds with probability p_{qubit}. A bit flip error occurs with probability p_{flip}.
- The creation of an EPR pair is attempted at a rate f_{EPR} and succeeds with probability p_{EPR}.
- The creation of an n-qubit GHZ state is attempted at a rate f_{GHZ-n} and succeeds with probability p_{GHZ-n}.
- The routing of a state received from a user to another one succeeds with probability $p_{transmit}$.
- A Bell State Measurement (BSM) on two photonic states received simultaneously succeeds with probability p_{BSM}.
- Photonic qubits are coupled in fibers with a probability $p_{coupling}$, also called coupling efficiency.
- Losses in optical fibers are characterized by the quantity η_{fiber} in dB/km, such that a photon is transmitted over a distance L with probability $\exp(-\eta_{fiber} \cdot L/10)$, and dephasing occurs with probability $p_{dephase}$.
- A photonic qubit is successfully measured with probability p_{det}, and the outcome is flipped with probability $p_{crosstalk}$.
- Detectors are active only in a time window Δt_{det} around each state creation attempt, called the detection gate.
- Detectors can spontaneously be triggered even in the absence of photons, resulting in dark counts at an average rate R_{dark}. Hence, they occur with a probability $p_{\text{dark}} = R_{\text{dark}} \cdot \Delta t_{\text{det}}$ when attempting to create a state. Dark counts typically trigger state detection, when none was emitted or when the state was lost. They can also lead to double outcomes at the detection of one qubit, in which case the data is discarded.

Other effects can occur with far lower probabilities and are therefore ignored.

In Fig. 5.2, we show as an example the error and loss model that we consider for sending and receiving a photonic qubit. It is a generalization of the loss model that was used in the previous chapter to model fiber communication (Fig. 4.6).

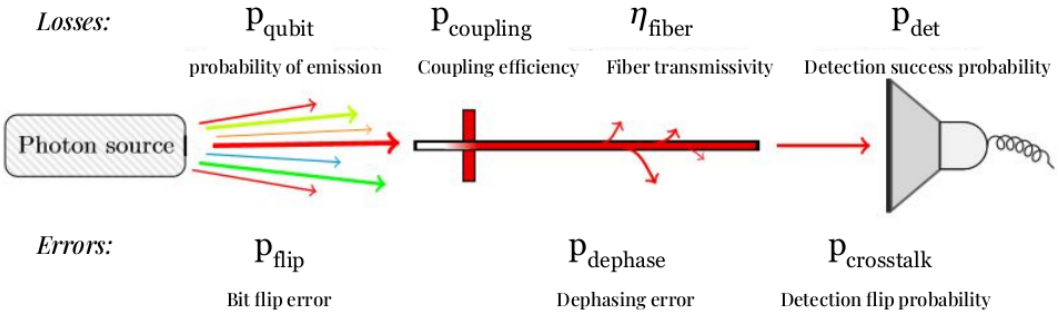


Figure 5.2: Photon loss and error model for the emission, sending and measurement of a qubit.

For modularity, all the failure probabilities and rates can be defined separately for each Qlient and for the Qonnector. This reflects the future probable differences in hardware quality between a server node and the different end users. Note that we here ignore the travel time of photons. We fix it to 1ns in our simulations, regardless of the distance between the nodes. In a real life setting, this travel time should be carefully measured so that receiving nodes know as precisely as possible when they should expect photons. This typically causes the receiving node to start its measurement routine a few milliseconds after the sending node starts sending photons, to account for photon travel time in the fiber.

To simulate our network architecture we use a quantum network simulation tool using discrete events, NetSquid [31]. Most errors and losses are embedded in Netsquid which facilitate the simulation of realistic quantum networks. The modularity of this simulator and its built-in components allows us to easily create a network model on which one can run protocols of interest. By defining simple local routines for each node such as the creation and sending of a state or performing a Bell state measurement, we can simulate the quantum operations involved in the protocols we consider. In this work we focus on modeling quantum operations and we do not take classical pre and post processing into account as their complexity is still sufficiently low to be performed fast enough by any classical computer. This will allow us to find the critical physical parameters of the Quantum City architecture that limit the functionalities accessible to a user, hence pointing to possible optimizations for networks under development. To learn more about the use of NetSquid, we encourage the reader to check out the NetSquid website [202]. The code used in our work is available on GitHub [203] and the documentation can be found in Appendix B.

5.1.3 Figures of merit

Using a network simulator allows to benchmark different properties of network protocols depending on specific hardware parameters. In this chapter we will focus on the **raw throughput**, in bit per second, at which protocols can be performed. As introduced in Sec. 4.4, the throughput is highly dependent on the quantum state creation rate of the sources which varies a lot from a setup to another and can usually be tuned to match the detector's dead time. We will also give an estimation of the **rate**, defined as the number of states received divided by the number of states sent (or channel uses). Although they can easily be converted from one to the other given the hardware parameters, the former gives a good estimate of the feasibility of a protocol while the latter characterizes the quality of the qubit transmission in a quantum network. Note that we here focus on the raw throughput instead of the secret key as we did in the last chapter because it applies to other protocols than QKD.

We will also focus on the **Qubit Error Rate (QBER)** that we define as the number of measurement outputs that where flipped during quantum processes. More explicitly it corresponds to the number of qubits measured in the $|1\rangle$ state when a $|0\rangle$ state was sent (and conversely) over the total number of qubits measured. This bit flipping due to faulty operations during the protocol is a practical measure of the quality of the different pieces of hardware.

These parameters allow in most cases to estimate the actual rate at which a protocol can be performed. For example in QKD protocols, the secret key rate is given as a function of the throughput and the QBER that depends on the post-processing techniques that are chosen [46]. Here, we focus on the quantum communication and processing parts of protocols, ignoring classical pre and post processing. Indeed, we simply aim to investigate the performances of a realistic near-term metropolitan-scale quantum network to motivate and guide practical implementations. Based on the results of our simulations, it will be then possible to check in more detail the feasibility of specific protocols. We hope this will show that the Quantum City is a promising architecture, suitable for near term quantum applications.

5.2 Results

We will now simulate a Quantum city in a realistic setting using Netsquid. As explained in Sec. 5.1.2, errors and losses are modeled with dephasing and depolarising channels that we apply to quantum states when they undergo quantum processes. Our simulation model is formed by five Qlients that represent actual laboratories in the Parisian region: Sorbonne Université campus (SU-Alice), Université Paris Cité campus (UPC-Bob), Orange Labs Châtillon (OR-Charlie), Télécom Paris (TP-Dina) and TGCC-CEA (CEA-Erika) (see Fig. 5.3). They are connected through lossy optical fibers to a Qonnector placed in the same lab as Alice. It is easy to see that this choice of placing the Qonnector is not optimal however it can allow for more Qlients at different distances to join and we will see that it already allows interesting applications.

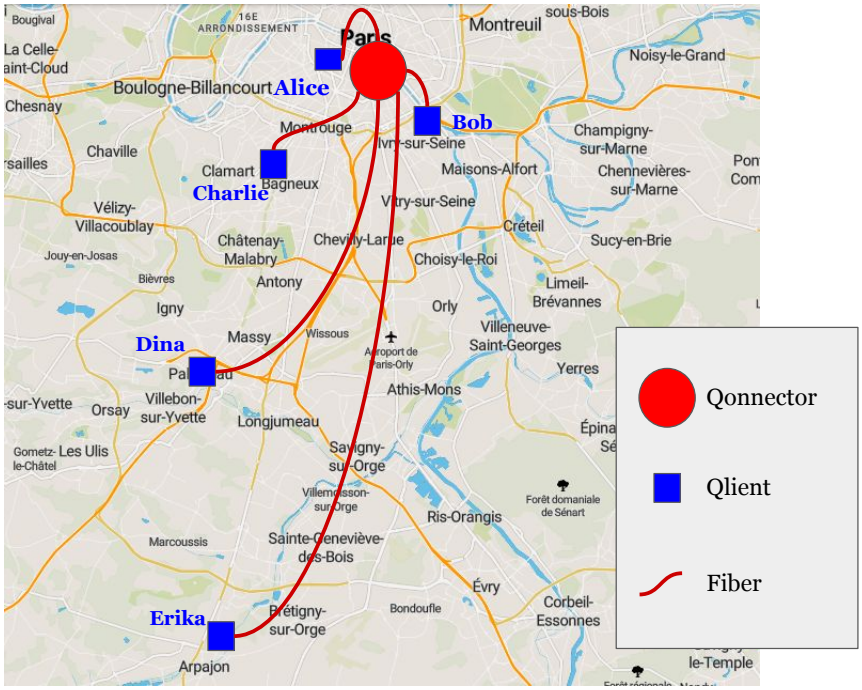


Figure 5.3: Paris Quantum City: Five Qlients are connected through optical fibers to a Qonnector located at Sorbonne Université (SU) campus. The length of the fiber are 1m for the link Alice-Qonnector, 3km for the link Bob-Qonnector, 7km for the link Charlie-Qonnector, 19km for the link Dina-Qonnector and 32km for the link Erika-Qonnector.

In Netsquid, protocols are modeled with node subroutines that correspond to the local operations performed by each node during the protocol. By creating the routines that correspond to creating and sending BB84 states, measuring such states in random bases, transmitting these states from one Qlient to another, creating Bell pairs or GHZ states and performing Bell State Measurement, we are able to simulate all the protocols mentioned in Sec. 2.1.1 and 2.2, at least from a network point of view. We also created classes of nodes that represents Qlients and Qonnector. They contain the necessary classical memory slots for routing and processing outcomes. Note that quantum storage is not included in the routines in this analysis. With these elements we can create a Quantum City instance on which all the protocols can be simulated.

5.2.1 Baseline simulation parameters

We start by discussing the set of realistic parameters that we use in our simulations. We consider here photon sources based on Spontaneous-Parametric Down-Conversion (SPDC) in nonlinear crystals, as they are widely used for generation of heralded single-photon and entangled-photon states with high performance in terms of brightness and fidelity [35, 34]. Such sources are in general cost-effective and can operate at a range of wavelengths. Note however that deterministic single-photon sources, such as those based on semiconductor quantum dots, may also be interesting for quantum network applications [204].

Using SPDC sources, heralded single-qubit states are generated by measuring one photon of a correlated pair with a single-photon detector. EPR pairs are generated with a probability p_{EPR}. Measuring one photon of an EPR pair with a single-photon detector allows us to herald its twin and therefore generate a single-photon state. GHZ state with $2n$ qubits are created by simultaneously generating n EPR pairs and performing on them probabilistic fusion operations [205]. We assume here that the probability of success of the fusion operation is the same as the one of a linear-optic BSM [206] with some additional losses, and set it to $p_{\mathrm{fusion}} = 0.36$. We therefore deduce the average generation rate for $2n$-qubits states:

$$GR_{2n} = f \cdot p_{EPR}^{n} \cdot p_{fusion}^{n-1} \tag{5.2}$$

with f the pump Laser repetition rate and we consider each Laser pulse as an attempt to create a state. This way, we can evaluate the probability of generating a GHZ state in a Laser pulse:

$$p_{GHZ-2n} = p_{EPR}^{n} \cdot p_{fusion}^{n-1}, \tag{5.3}$$

GHZ states with $(2n-1)$ qubits are generated by measuring a heralding qubit of a $2n$-qubit GHZ state, resulting in an average generation rate:

$$GR_{2n-1} = GR_{2n} \cdot \eta_{herald} = f \cdot p_{EPR}^{n} \cdot p_{fusion}^{n-1} \cdot \eta_{herald} \tag{5.4}$$

with η_{herald} the probability of measuring the heralding photon, including detectors and coupling efficiency, as well as eventual losses in optical components. For state-of-the-art detectors and optimized coupling setup we can consider $\eta_{herald} \simeq 0.7 - 0.8$. Similarly to the $2n-$qubits GHZ state case we can interpret f as the rates f_{qubit} and $f_{GHZ-(2n-1)}$, and we can evaluate the probabilities of generating a single-photon or a GHZ state in a laser pulse:

$$\begin{aligned} p_{qubit} &= p_{EPR} \cdot \eta_{herald} \\ p_{GHZ-(2n-1)} &= p_{EPR}^{n} \cdot p_{fusion}^{n-1} \cdot \eta_{herald} \end{aligned} \tag{5.5}$$

Most current experiments use Laser that do not exceed a pulse repetition rate of $f = 80\,\mathrm{MHz}$. Temporal multiplexing can be used to increase the average rate of emission while keeping the noise low [34]; however, we wish to keep $f \cdot p_{\mathrm{EPR}} \leq 10\,\mathrm{MHz}$, as a higher pair emission rate would lead to a drop of the detector performance because of the recovery time, which is typically $\lesssim 100\,\mathrm{ns}$. Hence, we take $f = 80\,\mathrm{MHz}$ and $p_{EPR} = 0.01$ for $1-$ and $2-$qubits experiments, in order to limit the noise due to double emission [207]. For experiments with more photons, we take a higher value $p_{EPR} = 0.1$ in order to favor multiple-pair emission in one pulse, while keeping a lower $f = 8\,\mathrm{MHz}$.

Below we list the parameters used for the simulations. Most of them are actual parameters witnessed in nowadays experiments, or are derived from what is expected to be possible in the years to come. Some others, such as the errors probabilities p_{flip}, $p_{crosstalk}$ or $p_{dephase}$, highly depend on how tailored the experiment is. We therefore choose somewhat arbitrary parameters, that can be easily modified in our code in order to simulate errors in the protocols. We also set somewhat arbitrarily the routing probability p_{transmit}, leaving the possibility to change it in order to model novel techniques. Hence we also set an arbitrary value for $p_{transmit}$, leaving the possibility to change it in order to model novel techniques. Finally, we set the parameters p_{det}, R_{dark}, and Δt_{det} to values corresponding to high-performance superconducting nanowire single-photon detectors.

Parameters:

f_{qubit}	80 MHz	Qubit creation attempt frequency
p_{qubit}	$8 \cdot 10^{-3}$	Success probability of creation of a qubit
p_{flip}	0	Flipping probability at the creation of a qubit
$p_{crosstalk}$	10^{-5}	Probability that the detector flips the outcome
f_{EPR}	80 MHz	EPR pair creation attempt frequency
p_{EPR}	10^{-2}	Success probability of the creation of an EPR pair
p_{BSM}	0.36	probability that a Bell state measurement succeed
f_{GHZ}	8 MHz	GHZ state creation attempt frequency
p_{GHZ-3}	$2.5 \cdot 10^{-3}$	Probability that an attempt of a 3 qubits GHZ state creation succeeds
p_{GHZ-4}	$3.6 \cdot 10^{-3}$	Probability that an attempt of a 4 qubits GHZ state succeed
p_{GHZ-5}	$9 \cdot 10^{-5}$	Probability that an initialisation of a 5 qubits GHZ state succeed
$p_{transmit}$	0.9	Probability that transmitting a qubit succeeds
t_{gate}	1 ns	Time it takes to perform an operation on one qubit
$p_{coupling}$	0.9	Fiber coupling efficiency
η_{fiber}	0.18 dB/km	Fiber loss per kilometer
$p_{dephase}$	0.02	Phase flip probability in the fiber
p_{det}	0.95	Detector efficiency (Probability that a measurement succeeds)
R_{dark}	100Hz	Dark count rate
Δt_{det}	100 ps	Detector detection gate

5.2.2 Bipartite protocols

5.2.2.1 Simulation of Quantum Key Distribution protocols

Here, we show the performance of the Quantum City architecture for Quantum Key Distribution. Our analysis uses as a running example a quantum network in the Paris region (see Fig. 5.3), featuring characteristics common to many urban areas in Europe and beyond. As shown in Sec. 2.1.1, there are many protocols achieving the QKD functionality, namely establishing a secret key between two Qlients. These protocols differ in rate, hardware involved and in the trust that Qlients give to the Qonnector. In the context of this work, we suppose that each Qlient node is capable of manipulating (creating and/or measuring) one qubit at a time. The Qlients choose among the different QKD protocols depending on their hardware or on which feature is more desired. In Fig 5.4, we show five QKD protocols between two Qlients that we study in the following.

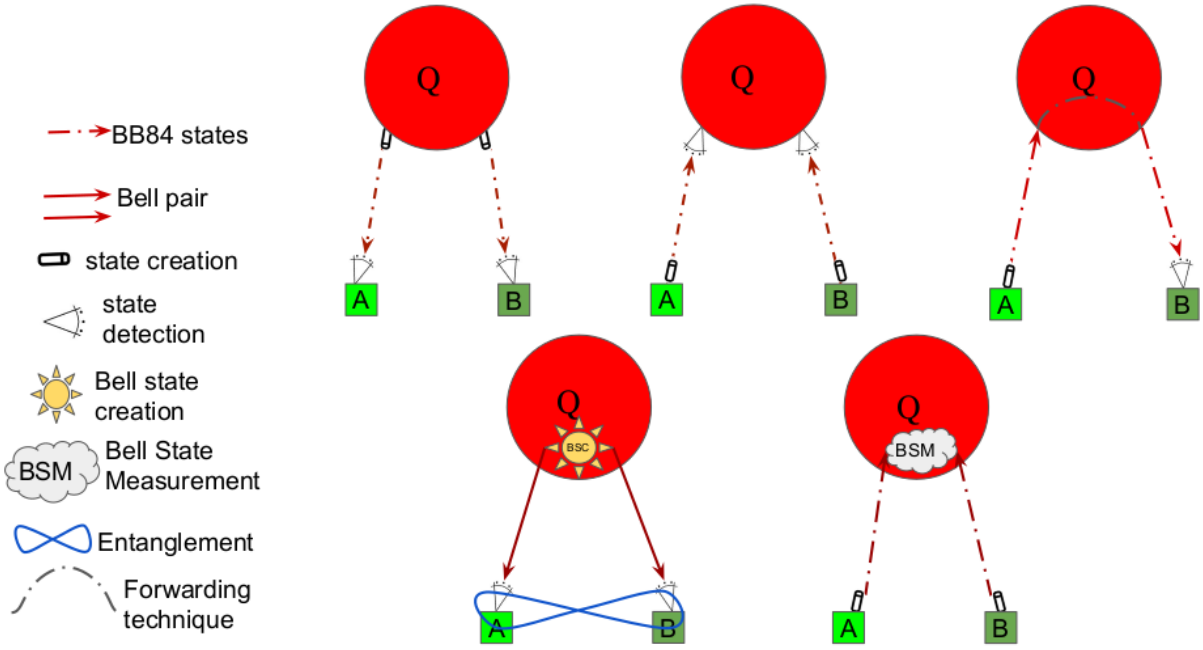


Figure 5.4: QKD protocols between two Qlients of a Quantum City. From left to right, top to bottom: 2xBB84, 2xBB84 reversed, transmitted BB84, Entanglement-based QKD and MDI-QKD. The hardware involved in each of these protocols is given on the left.

We perform between 200 and 500 simulation runs for each protocol. By averaging over these runs, we give an estimate of the sifted key throughput by dividing the length of the sifted key over the simulation time. We estimate the rate by dividing the number of photon received by the number of photon sent as well as the QBER by counting the number of bits that have been flipped at the end of protocol. We also show plots with the accumulated sifted key after a certain simulation time. Sifted key rate and QBER are the two main parameters taken in consideration during the calculation of the secret-key rate of QKD protocols.

BB84. We first simulate the performances of the BB84 protocol (see Sec. 2.1.1.1 for details) in two settings: between the Qonnector and each Qlients and between two Qlients using the Qonnector as a router. In the first case, once a key is shared between the Qonnector and two Qlients, the Qonnector can use one Qlient's key to transmit him the other Qlient's key. We assume for the moment that all the nodes have the same hardware parameters so it does not matter whether the sender is the Qonnector or the Qlient. In the second case, the photon transmission at the Qonnector node succeeds with probability $p_{\text{transmit}} = 0.9$; we recall that this routing parameter can easily change in the simulation.

The simulation is performed as follows: At each timestep defined by $1/f_{qubit}$ as the time necessary to create a BB84 state, a photon is created at a sending node. The associated classical bit as well as the basis and a timestamp are stored in classical memory slots. Qubit states are sent through fibers along with a classical message containing the timestamp. They are then measured at the receiving node and outcomes are stored in classical memory slots alongside the measurement basis and the timestamp. After a fixed simulation time, we perform sifting on the two resulting lists, using the timestamps to compare measurement basis accordingly. This leaves us with correlated lists of raw key bits at the sending and receiving nodes from which we can extract data of interest for our analysis.

In Table 5.1 we show the achieved sifted key throughput, rate and QBER after a few hundred rounds of simulation. We also show in Fig. 5.5 the throughput for each Qlient as a function of the distance and in Fig. 5.6 and 5.7 the number of successful BB84 round as a function of the simulation time for each setting.

Nodes involved	Throughput (sifted key bit per second)	Rate (sifted key bit per channel use)	QBER
Qonn $->$ Alice	263900	0.423	1.0%
Qonn $->$ Bob	228700	0.374	0.9%
Qonn $->$ Charlie	200700	0.322	1.0%
Qonn $->$ Dina	116850	0.180	0.9%
Qonn $->$ Erika	71250	0.115	0.9%
Alice $->$ Qonn $->$ Bob	184200	0.2185	1.8%
Alice $->$ Qonn $->$ Charlie	158450	0.2592	1.8%
Dina $->$ Qonn $->$ Charlie	72700	0.1078	1.9%
Bob $->$ Qonn $->$ Erika	51950	0.0845	1.7%

Table 5.1: Performance of the BB84 protocol in the Paris Quantum City. The first five lines correspond to the Qonnector sending BB84 state to each Qlient, and the last four correspond to pairs of Qlient using the Qonnector as a transmitting station.

The actual key rate that corresponds to sharing a key between two Qlients using the BB84 protocol between the Qonnector and the Qlients is given by the minimum of the key rate with each individual Qlient. As expected, photon loss in the fiber affects directly the performance of this protocol. We can see the rate dropping for nodes situated further away from the Qonnector, dropping even more when the Qonnector routes a photon coming from one Qlient to another. Despite this lower performance, Qlients do not have to trust the Qonnector in the latter case. They can see if it is tampering with the state they are sending during the reconciliation part of the protocol.

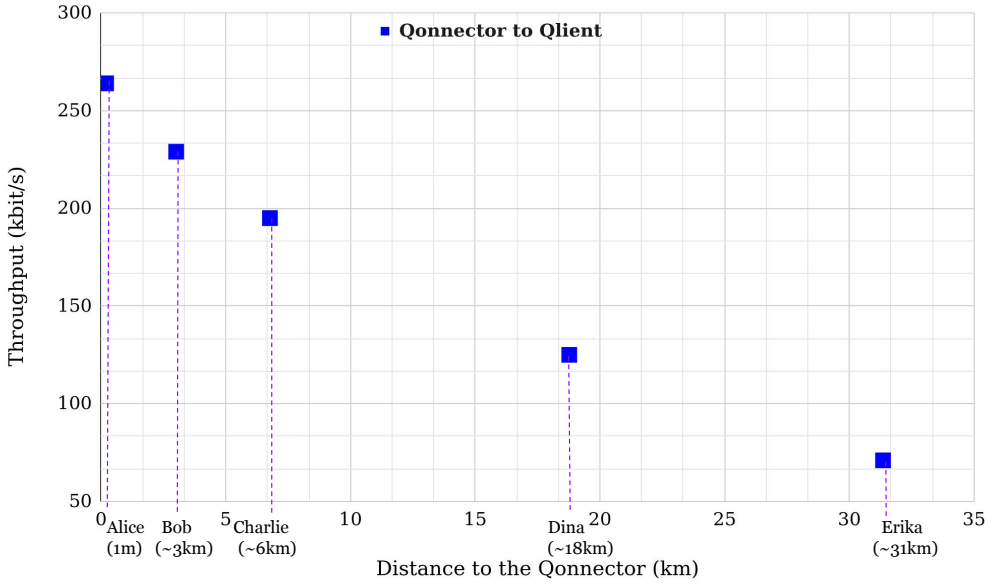


Figure 5.5: Throughput of BB84 state transmission from the Qonnector to the Qlients (blue squares). The throughput is the number of sifted key bits per second shared between each Qlient and the Qonnector.

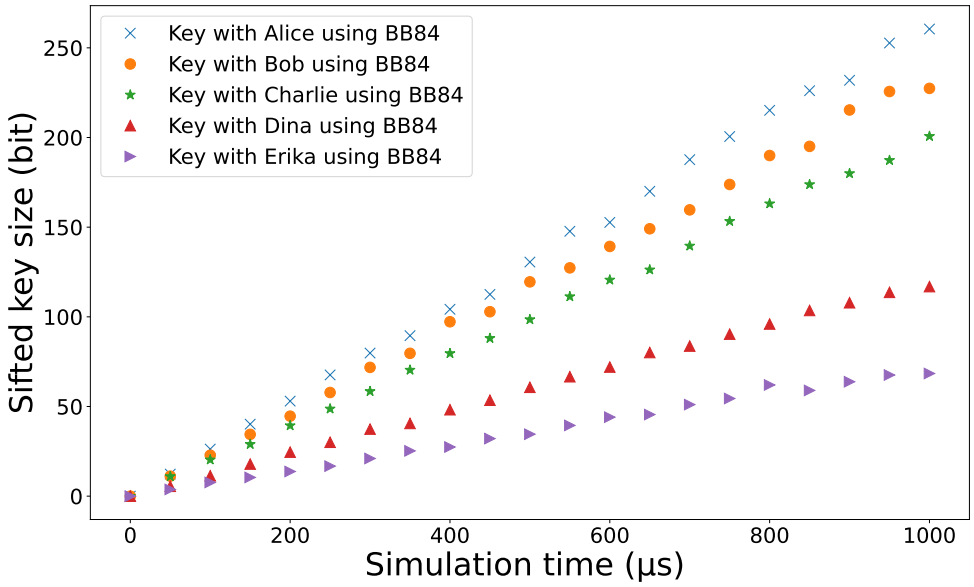


Figure 5.6: Comparison between the number of successful BB84 qubit transmission from the Qonnector to every Qlient of our network.

As a comparison [208], BB84 experiment done using nitrogen-vacancy defect centers as single photon sources with 1MHz repetition rate at a few meter distance in free space gives lower sifted key throughput of 3.99kbit/s while the ones with silicon-vacancy defect center have a sifted key throughput of 1.51kbit/s.

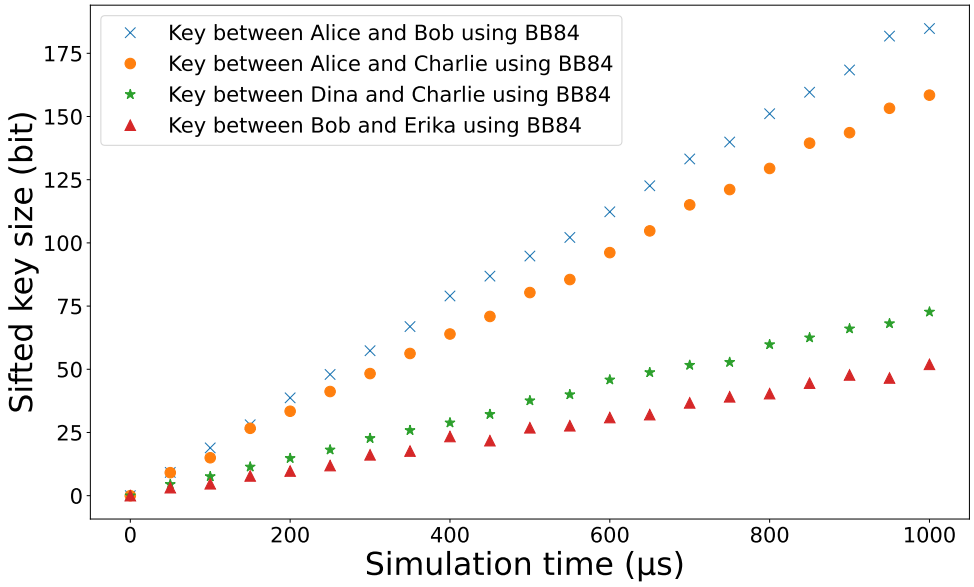


Figure 5.7: Comparison between the number of successful BB84 qubit transmission from some Qlients to others through the Qonnector.

Entanglement-based QKD. We now investigate the performance of the Quantum City for QKD when EPR pairs are sent between Qlients. We simulate the following: at each timestep defined by $1/f_{\text{EPR}}$ an EPR pair is created and sent by the Qonnector to two Qlients who measure it in a randomly selected basis according to the protocol. As in the BB84 simulations, outcomes, timestamps and measurement bases are stored in classical memory slots. We can then use the resulting lists to extract relevant data. Note that to estimate the QBER we count the timesteps where Qlients obtained correlated results.

In Table 5.2 we show the EPR sharing rate and throughput as well as the QBER for a few pairs of Qlients. We also plot in Fig. 5.8 the accumulated sifted key obtained by pairs of Qlient receiving and measuring EPR pairs from the Qonnector and counting the qubits received with the same timestamp and measured in the same basis.

Nodes involved	Throughput (EPR pair per second)	Rate (pair received over pair sent)	QBER
Alice $<-$ Qonn $->$ Bob	248250	0.2068	1.9%
Alice $<-$ Qonn $->$ Erika	79750	0.1042	1.3%
Dina $<-$ Qonn $->$ Charlie	96750	0.1252	2.2%

Table 5.2: Performance of the BBM92 protocol between pairs of Qlients

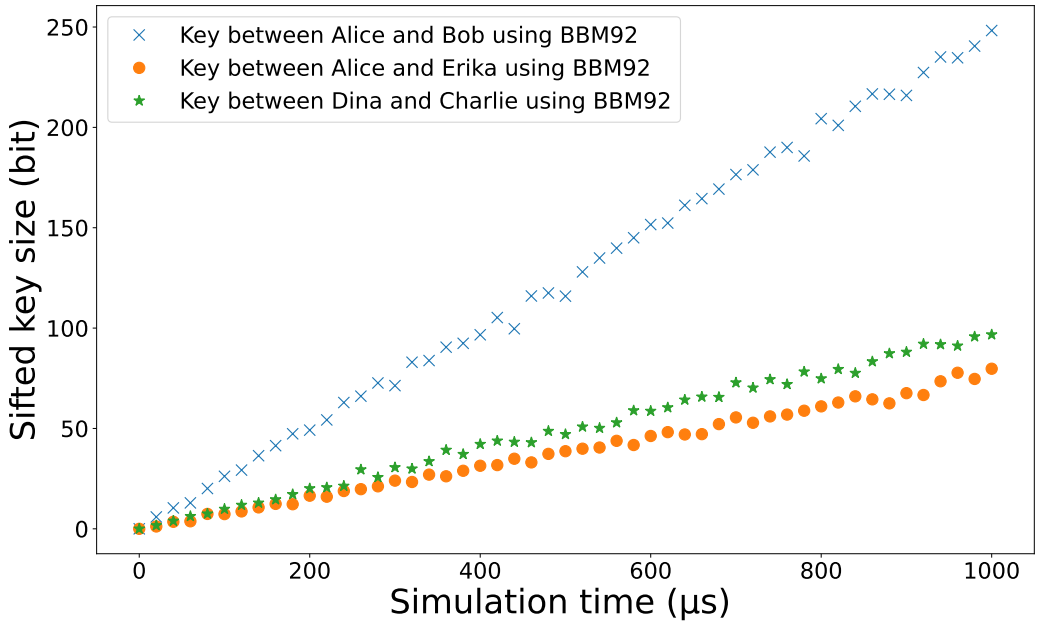


Figure 5.8: Comparison between the number of EPR pairs successfully measured by pairs of Qlients.

Note that this also showcases how long it takes to create entanglement between two nodes in the Quantum City. As explained in the introduction, this is a crucial characteristic of a quantum network. To consider this properly, it is necessary to upgrade the Qlient capacities with quantum storage. In addition to allowing for efficient, on-demand operations, this also opens the way to a whole range of applications based on teleportation and entanglement swapping techniques.

MDI-QKD. Finally we simulate the MDI-QKD protocol as follows: at each timestep the Qlients prepare and send BB84 states to the Qonnector who performs a Bell state measurement on them (see Sec. 2.1.1.3 for details). If the measurement is successful, the outcome along with its timestamp is stored in a classical memory slot. We do not simulate classical post-processing and consider that a round is successful when the joint BSM is successful. As these techniques are still under development, we will only give an estimation of the protocol's rate in order to compare to other protocols. In particular, we will leave the consideration of noise and dark counts in the Bell State measurement as an open question. We show the performance of MDI QKD between two different Qlients in Table 5.3.

Qlient involved	Throughput (successful MDI QKD round per second)	Rate (successful round over photon sent)
Alice $->$ Qonn $<-$ Bob	420	0.05%
Alice $->$ Qonn $<-$ Charlie	330	0.04%
Dina $->$ Qonn $<-$ Charlie	240	0.03%
Bob $->$ Qonn $<-$ Erika	30	0.004%

Table 5.3: Performance of the MDIQKD protocol between pairs of Qlients

The low success probability of the Bell state measurement combined with low probability that both Qlient photons arrive at the same time explains the lower rate of this scheme compared to the previously studied schemes. However, this scheme could be greatly improved by using quantum memories to store an arriving qubit from one Qlient for a small time until a qubit arrives from the other Qlient [209]. Moreover, MDI QKD has strong security properties as Qlients do not need to trust the Qonnector. It might be preferred over the BBM92 protocol for hardware considerations: high-quality detectors typically involve cryostats that may be too expensive for Qlients.

Moreover research in variants of this protocol is evolving rapidly, especially with the rise of novel Twin-Field QKD techniques exploiting new phase locking techniques [54]. We leave the modeling of this particular QKD protocol to further work. For now we simply showcase the feasibility of MDI-QKD in a Quantum City architecture.

We conclude this section by noting that **decoy-state BB84** [210] and Continuous-Variable QKD or **CV-QKD** [61, 211] are also widely studied QKD protocols offering significant advantages (see Sec. 2.1.1.4). Unfortunately, NetSquid does not support yet models for (weak) coherent state generation or coherent detection techniques used in these protocols, and therefore we do not include them in our analysis. We emphasize, however, that it will be important to develop such network simulation models for a complete analysis of quantum networks, and leave this as an open question.

5.2.2.2 Playing with the parameters

To test our network architecture in the most realistic setting, we can choose different capabilities for each node. As an example let us set Bob to have the best detector parameters but a low-performance transmitter ($p_{\text{qubit}} = 5 \cdot 10^{-3}$ and $p_{\text{flip}} = 0.01$) and Dina to have the best transmitter parameters but low-performance detectors ($p_{\text{det}} = 0.85$, $p_{\text{crosstalk}} = 10^{-2}$, $R_{\text{dark}} = 10^4$Hz and $\Delta t_{\text{det}} = 500\,\text{ps}$). Moreover, let Charlie represent the most limited Qlient with the lowest abilities both in sending and detecting states. We leave the Qonnector as well as Alice and Erika to have the best possible choice of parameters that corresponds to state of the art capabilities. We emphasize that all these parameters can be easily modified in our code and that the simulation modules are available on GitHub[203]. In this section, we will refer to this more realistic set of parameter as the modified set of parameters.

In Table 5.4 we show the sifted key rate, throughput and QBER for sending and receiving BB84 state both ways between the Qonnector and each Qlient. We also plot the rate as a function of the distance between the Qonnector and each Qlient (see Fig. 5.9). We see that the different quality in hardware directly reflects on the simulations outcomes. For example, Bob, who has state of the art detectors but poor transmission capabilities, performs better as a receiving node, and Dina, with the reverse capabilities, performs better as a sending node. We remark that with the simulation parameters we have chosen, the effect of the transmitting capability is more pronounced that the detection one.

Nodes involved	Throughput (sifted key bit per second)	Rate (sifted key bit per channel use)	QBER
Qonn − > Alice	263900	0.4233	1.0%
Qonn − > Bob	228700	0.3742	0.9%
Qonn − > Charlie	175650	0.2864	1.9%
Qonn − > Dina	112050	0.1804	2.2%
Qonn − > Erika	71250	0.1156	0.9%
Alice − > Qonn	260450	0.4323	1.0%
Bob − > Qonn	141800	0.3735	2.0%
Charlie − > Qonn	122400	0.3218	2.0%
Dina − > Qonn	121750	0.1963	1.0%
Erika − > Qonn	70750	0.1142	0.9%

Table 5.4: Performance of the BB84 protocol between Qlients and the Qonnector in the Paris Quantum City with the modified set of parameter.

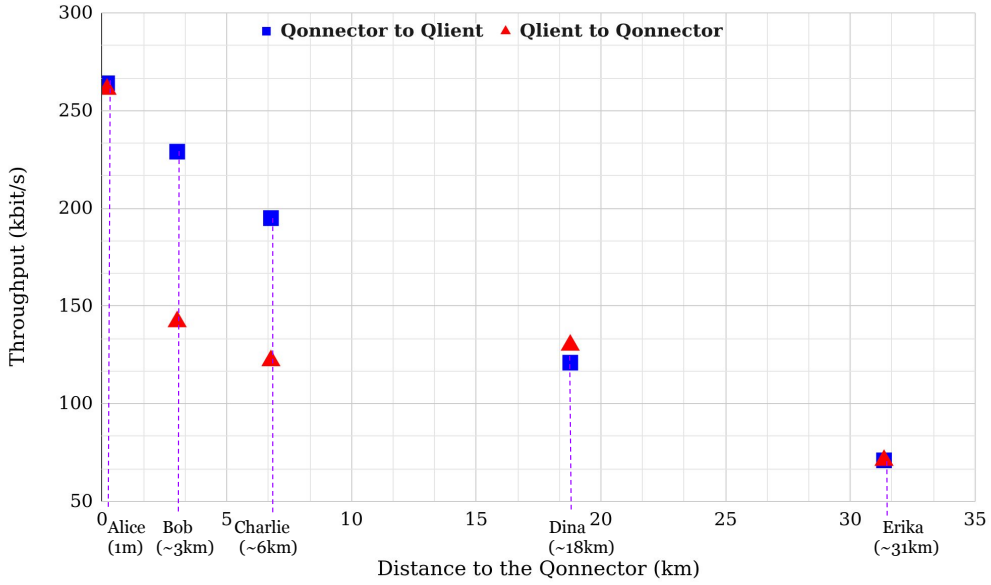


Figure 5.9: Throughput of BB84 state transmission from the Qonnector to the Qlients (blue squares) and from the Qlients to the Qonnector (red triangles) with the modified set of parameter. The throughput represent the number of sifted key bits per second shared between each Qlient and the Qonnector.

We have studied the feasibility of different QKD protocols from Sec. 2.1.1 in a realistic Quantum City architecture. With simple optical elements on the Qlient side, we have seen various ways for two Qlients to secretly share a key that we can now compare. In Figs. 5.10 and 5.11 we show the accumulated sifted key length as a function of the simulation time for different QKD protocols for Alice and Bob and for Charlie and Dina with the modified set of hardware parameters. With these parameters, we can see that Alice and Bob can use favorably entanglement-based QKD while BB84 from the Qlients to the Qonnector is optimal for Charlie and Dina. For these small simulation times, MDI-QKD generates few bits of shared key due to its very low success probability, which appears as zero when averaging over all the simulation runs. This highlights that such network simulation tools can allow in a fast and flexible

way for resource optimization when choosing between different protocols for a target functionality, while also considering a the trade-off between performance and desired trust requirements.

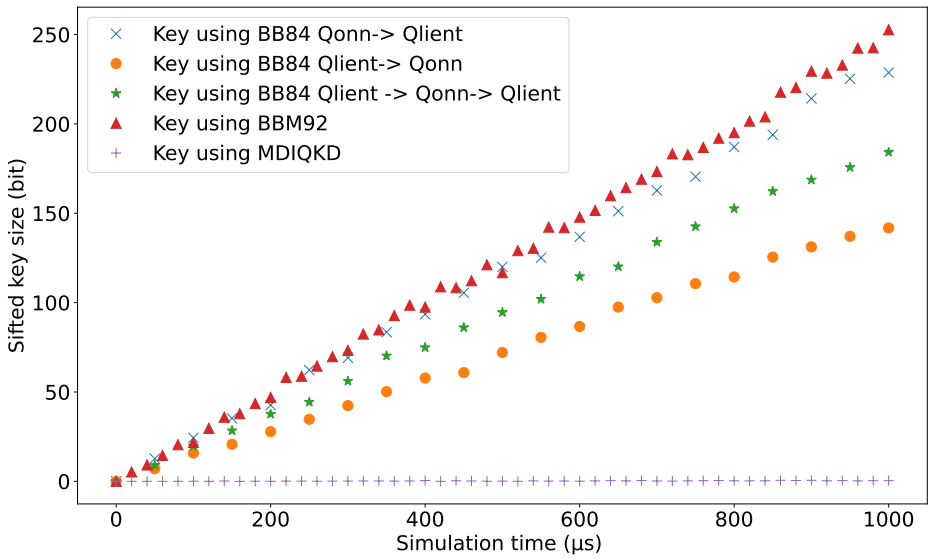


Figure 5.10: Comparison between different QKD protocols between Alice and Bob. We show the size of the sifted key between the two Qlient using different QKD protocol as a function of the simulation time.

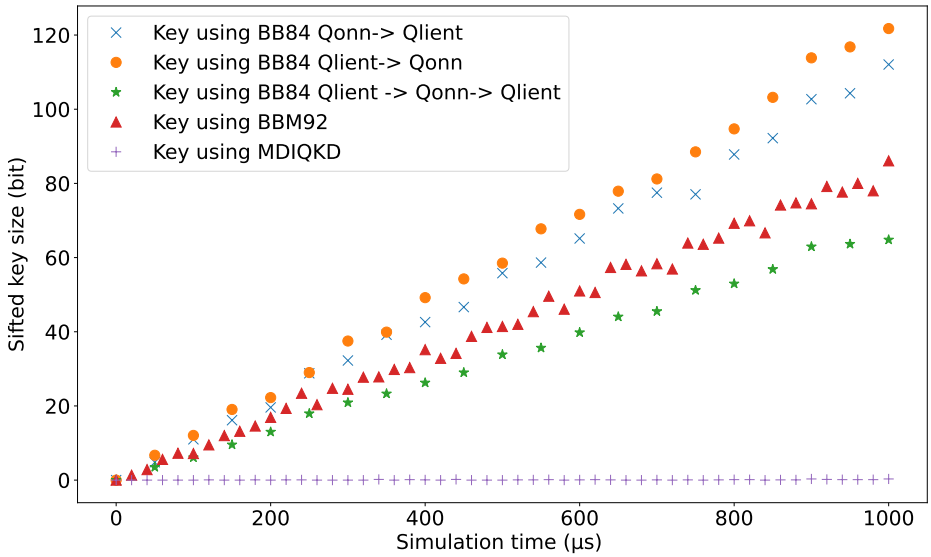


Figure 5.11: Comparison between different QKD protocols between Charlie and Dina. We show the size of the sifted key between the two Qlient using different QKD protocol as a function of the simulation time.

5.2.2.3 Delegated computation

In this section, we call a Qomputer node a node with access to a universal quantum device able to perform arbitrary computations. In the Quantum City architecture, simply connecting a Qomputer node to the Qonnector makes delegation protocols available to any Qlient. The Qomputer could for example work in the measurement-based quantum computing paradigm [82] where a computation is done by successive adaptive measurement on a grid of entangled qubits. Delegation can be done by asking the Qlient to send a photon whose phase is randomized then with a back-and-forth classical interaction (see Sec.2.1.4 for more details). In this work we will not dive into the details of how the qubits are entangled and measured by the Qomputer, but rather estimate the rate at which they can be sent from the Qlient to the Qomputer. Although we don't expect near-term Quantum Cities to have a Qomputer node, this showcases the feasibility of delegated computation protocols from a network point of view.

Let us imagine that one of the nodes of our quantum City, say Erika, grows to have the abilities of a quantum computer and becomes a Qomputer node. As explained in Sec. 2.1.4, by simply sending single photons and then classically communicating with Erika, any Qlient of the Quantum City can enjoy Erika's quantum computing power. In Table 5.5 we show the throughput at which single photons can be sent from each Qlients to Erika with our baseline set of parameters.

Qlient	Throughput (successful photon transmission per second)
Alice	118200
Bob	64940
Charlie	54480
Dina	53520

Table 5.5: Performance of qubit transmission from each Qlient to Erika through the Qonnector.

We do not know yet how this rate relates to the rate of the actual computation a Qlient could perform. However the work from [212] shows that the method that we have described in Sec. 2.1.4 comes within a factor of 8/3 of optimal in the used resources. This means that in principle, new developments could reduce the number of photons sent necessary to remotely perform an operation. The optimization of delegation protocols, which also depend on the Qomputer technology and computing model, is outside the scope of this thesis. Note also that according to the results from [79], a Qlient could even securely use the Qonnector to send qubits to Erika and delegate a quantum computation while being completely classical.

5.2.3 Multiparty protocols

As discussed in Sec.2.2, most interesting applications of quantum networks are multiparty computations taking advantage of shared multipartite entanglement. In a Quantum City architecture, multiparty protocols that only require a qubit per party at each timestep can be implemented.

In this work we focus on protocols based on the GHZ state $\frac{|0\rangle^{\otimes n}+|1\rangle^{\otimes n}}{\sqrt{2}}$ [5] such as the one presented in Sec. 2.2. However the Quantum city architecture allows for sharing any multiparty quantum state as long as at each timestep of the protocol only one qubit is held by each party. The Qonnector in this case is simply used as a source of genuine multipartite entanglement (see Fig. 5.12). Restricting our network simulation analysis to GHZ states, the relevant figure of merit for assessing the performance in this case is the rate of successful transmission of such states. Protocols using other states are not very different from a network simulation point of view; the main difference would be the probability that they are successfully created.

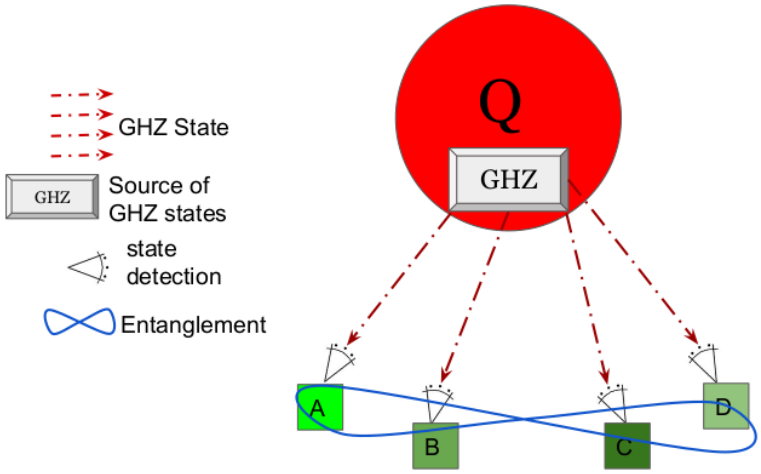


Figure 5.12: Sharing of a 4 qubit GHZ state from the Qonnector to Qlients.

Following the analysis of Sec. 5.2.1, we assume that n-qubit GHZ states are generated at the Qonnector node at a rate f_{GHZ} with a probability $p_{\mathrm{GHZ}-n}$. The qubits are then sent through the channels to the Qlients, who record the number of detection events. Precise synchronization is required for correctly assessing the obtained correlations. Here for simplicity, we just consider the events that correspond to the same timestamp.

We present in Table 5.6 the estimated sharing throughput and error rate for GHZ sharing in a Quantum City with the baseline set of parameters. The error rates have been estimated by counting the number of GHZ states successfully shared in which at least one of the outcome bits has been flipped during the process. For GHZ-5 the number of successful GHZ state transmissions is too low to have a correct estimation of the error rate.

We also show in Fig. 5.13 the number of GHZ states that arrive successfully to 3, 4 or 5 Qlients as a function of the simulation time. This may correspond, for instance, to accumulated raw conference key,

which can then be made secure following a conference key agreement protocol (see Sec. 2.2.2). We can see that scaling GHZ states to a larger size with the fusion operations considered in our simulations is challenging; going from 3 and 4 qubit GHZ states to 5 and 6 qubit GHZ states requires the operation to succeed twice, which occurs with low probability. Upgrading to techniques based on deterministic single-photon sources may offer a promising avenue towards such scaling [213].

Qlients involved	Throughput (successful GHZ shared per second)	GHZ error rate
GHZ3 to Alice, Bob and Charlie	4260	2.1%
GHZ4 to Alice, Bob, Charlie and Dina	4495	1.8%
GHZ5 to Alice, Bob, Charlie, Dina and Erika	45	-

Table 5.6: Performances of GHZ sharing from the Qonnector to 3, 4 and 5 Qlients.These results have been obtained after averaging over 500 runs of 2000μs.

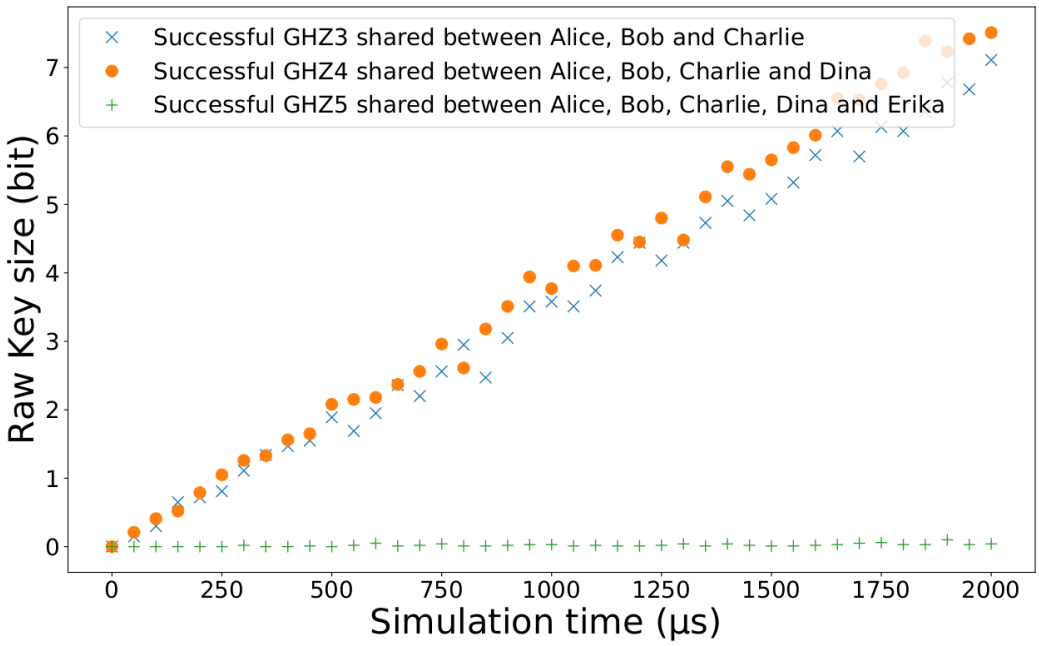


Figure 5.13: Number of GHZ state successfully transmitted to three, four and five Qlients as a function of the simulation time. It also corresponds to raw conference key size in a CKA context. Each point has been averaged over 100 runs of simulation.

These estimations of course highly depend on the GHZ creation rate of the source at the Qonnector node. As explained in Sec. 6.2.1, photonic GHZ states are created by applying fusion operations to Bell pairs. This explains why the number of GHZ states received by 3 and 4 parties are close. However, fusion-based GHZ creation scales quite badly with the size of the state. Going from 3 and 4 qubit GHZ states to 5 and 6 qubits GHZ state requires the probabilistic EPR fusion operation to succeed twice which is still very challenging today. Performing GHZ-based network applications with a number of Qlients above these numbers unfortunately seems unrealistic even with today's state of the art photonic hardware. However other methods using for example better single-photon sources are under investigation to push this limitation [36].

Once GHZ states are shared, multiparty quantum protocols such as conference key agreement or anonymous transmission become available to Qlients. When running, for instance, conference key agreement, the Qlients may not trust that the source is indeed providing GHZ states. The Qonnector may be dishonest or have noisy hardware. In this case, the Qlients will perform several verification rounds in between actual protocol rounds. Following the discussion in Sec. 2.2.1, it would take approximately 50 seconds for 4 Qlients to obtain one state such that there is a probability 0.99 that the state has 90% fidelity with the GHZ state. By randomly doing key agreement rounds in between tens of thousands verification rounds, four Qlients thus can perform a conference key agreement protocol secure against a malicious Qonnector in a few tens of minutes. They would then get a raw key from which a common secret key can be extracted. Hence, in a Quantum City with currently available hardware, secure 4-party conference key agreement protocols can be achieved in a relatively practical amount of time.

Similarly, the full anonymous message transmission protocol from [93] supposes that the protocol presented Sec. 2.2.3 is done in between GHZ verification rounds. This means that a message of a few bits can be securely and anonymously transmitted in less that an hour in our Paris Quantum City setting when 4 Qlients are involved. However, the time it would take to perform these protocols for more Qlients becomes impractical with present technology because of the low probability of n-qubit GHZ state generation when $n > 4$ and of the high overhead in GHZ states required by the verification protocol. Nevertheless if the Qlients choose to trust their Qonnector, the rate at which the presented protocol can be performed becomes quite practical. We can then conclude that near-term multiparty quantum protocols will most probably have to work in a trusted-node scenario.

5.3 Conclusion

In this chapter, we have presented a simple network architecture that is sufficient and realistic for metropolitan area quantum networks, of radius up to a few tens of kilometers. This architecture consists of a single powerful node with the ability to create bipartite or multipartite entanglement and make joint measurements in pairs of qubits, called the Qonnector, and a number of users with simple photonic capabilities of preparing and measuring single qubits, called the Qlients. Together they form a Quantum City. We have shown through Netsquid simulation the feasibility of various QKD protocols as well as some multiparty functionality. The code is available on GitHub [203] and the documentation can be found in Appendix B.

Our work gives rise to a number of open questions. Notably, we did not consider quantum memories in the nodes of our Quantum city. Integrating this aspect is of particular interest as it will allow for efficient routing strategies between the Qlients and for on-demand operations. Synchronization and timing strategies that need to be put in place at the nodes were also not discussed, and are crucial for proper network operation and hence for a complete protocol analysis. It will also be important to extend NetSquid to support the simulation of coherent state generation and coherent detection techniques to allow the investigation of an even wider range of protocols and applications. Finally, we also did not consider the effect of noise such as dark counts in Bell state measurements. Future work will also include more detailed error models for some of the protocol operations.

Our focus here has been to explore what applications can be available with optimized and realistic resources to quantum network users today. Our results highlight the significance and relevance of early deployment of quantum networks, while also preparing the ground for applications that will become available when more advanced quantum hardware is integrated, thereby unlocking the full potential of a Quantum Internet. Indeed, Quantum Cities could be linked together using quantum repeaters or free-space links, in order to create a larger-scale quantum communication network. The photonic and centralized features of the Quantum City architecture facilitates connectivity between different cities. It is capable of adapting with future developments on local nodes, provided efficient interfaces between photon and local quantum memories are developed. In the next Chapter we study the feasibility of satellite quantum communication to connect Quantum cities.

Chapter 6

Long distance communication

In Chapter 4, we saw that a successful implementation of quantum repeaters has not yet been demonstrated. Despite the promising simulation results of Chapter 5 on metropolitan scale quantum networks, communications beyond a city is crucial to achieve a Quantum Internet. Over the last decade, free-space communications and more particularly satellite communications have received more and more attention to overcome the issue of long-distance communications. Indeed in free-space, photons are less likely to be lost than in fibers especially if part of the photon path is outside of the Earth atmosphere. Feasibility studies [214] and actual implementations over more than 4000km [6] show that satellite quantum communication could be the missing link to interconnect the various metropolitan quantum networks that are being developed.

Contribution and outline: In this chapter, we continue the study started in Chapter 5 by simulating free-space links between two quantum cities. In Sec 6.1, we first design and provide a loss model for satellite to ground communication and for horizontal free-space communication. This modelling was done with the help of Matteo Schiavon and Valentina Marulanda Acosta. In Sec. 6.2, we then show and study the effect of different parameters on satellites sending single photons to ground stations using an adapted Netsquid library and real satellite orbital data. We then embed this study in the context of our Quantum Internet architecture by studying two QKD scenarios between different Quantum Cities in Sec. 6.3. Finally we discuss how realistic satellite communication is on the path towards quantum Internet in Sec. 6.4 where we also discuss and simulate a high-altitude balloon based alternative to achieve long distance communication.

Article link: The manuscript will be submitted within the next few weeks.

6.1 Connecting Quantum Cities with satellites

In this work we investigate the feasibility of a satellite-based international network architecture in a realistic pan-European context. In Fig 6.1, we show our envisioned network architecture, that we call the Qloud. It allows growth and adaptability to future developments and also minimizes the end user hardware which, as we saw in the previous chapter, is key for a practical implementation. It is based on satellite communication between Quantum cities that are small star-like metropolitan networks. Quantum cities centralize the information in so-called Qonnector nodes to optimize routing of quantum data between distant nodes. The full definition of each component of the Quantum City architecture can be found in Chap. 5.

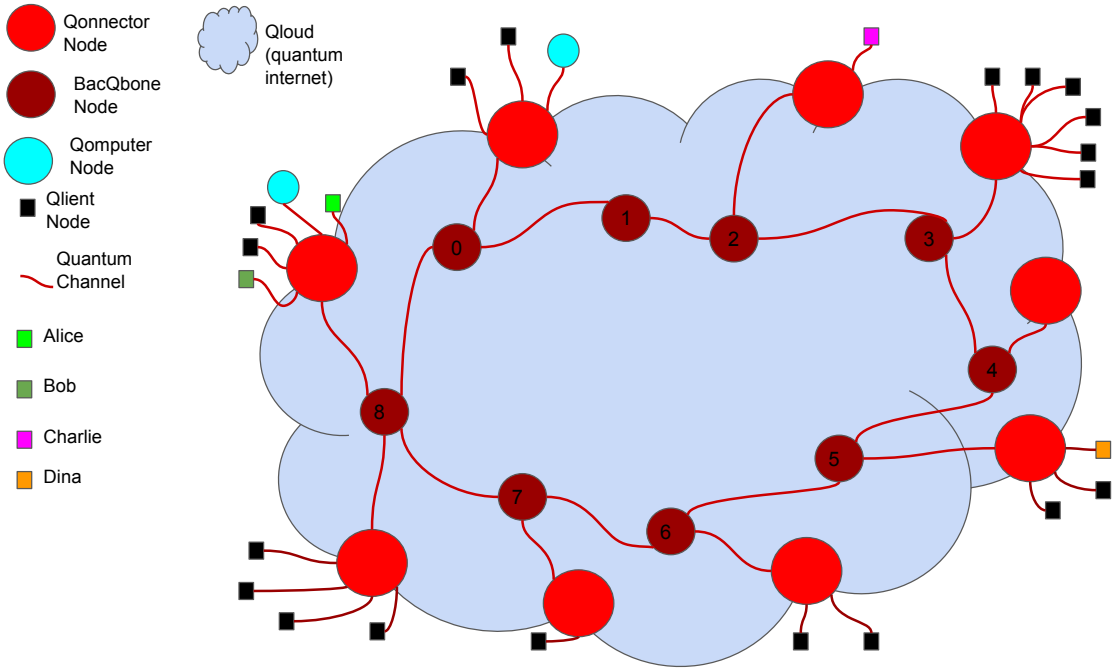


Figure 6.1: Schematic of a Qloud: Quantum cities connected through a backbone network of satellites (BacQbone nodes). A Quantum City is formed by a powerful central node (Qonnector nodes) used as a server allowing end users (Qlients) to enjoy quantum-enhanced functionalities. The end users can also be powerful quantum machines (Qomputer nodes).

We support this architecture with simulations that show the feasibility of quantum key distribution using real satellite data. We exhibit the crucial parameters by looking at their separate effect on the key rate of a simple BB84 downlink scenario and in different QKD settings. Note that the beam-wandering effect is stronger in the uplink scenario because the beam pass through the atmosphere at the beginning of the path, when it is of smaller size. Satellite communication is easier to implement from the satellite to the ground than the other way around. In the downlink scenario, the atmosphere comes at the end of the path. Hence, turbulence induced by the beam wandering due to the atmosphere has a much lower effect in this case. In the following we detail our model for the noise in satellite to ground quantum communication. This model has been created in collaboration with Valentina Marulanda Acosta and Matteo Schiavon.

Since atmospheric turbulence is a very complex phenomenon, the realisation of a model for it requires a choice of the effects that most severely affect the transmission. We have decided to focus on atmospheric absorption and beam wandering effects.

In order to describe the impact of atmospheric propagation on the signal, we exploited a computer code called Lowtran [215]. It is a fortran code developed for the calculation of the transmittance and background radiance of the atmosphere. It is based on an empirical prediction scheme derived from lab measurements and provides a reasonably accurate estimation of atmospheric effects over a broad spectral interval ($\sim$ 0.25 to 28.5 μm). The atmosphere is represented by 33 horizontal layers between sea level and an altitude of 100 km. The total transmittance is computed as the product of different atmospheric effects, namely continuum absorption, aerosol extinction, molecular scattering and molecular absorption, the latter of which includes the influence of water vapor, ozone, nitric acid and other uniformly mixed gases. The program contains a few different representative atmospheric models based on geographical-seasonal characteristics (such as for tropical or mid-latitude environments) that encompass the variation of pressure, temperature, water vapor and ozone with altitude. It also accounts for several aerosol models that describe particular meteorological ranges such as an urban environment, a less severe rural setting or a more wind and humidity dependent maritime navy situation. Lastly a couple of different visual ranges corresponding to different aerosol density models are considered as well [216].

In order to account for beam wandering, we used the model proposed by Vasylyev et al. [217] which presents a rigorous treatment of beam wandering effects, one of the leading causes of losses in the free-space channel. Its main advantage lies in an analytical formulation of the probability distribution of the transmission coefficient (PDTC), a feature exploited to provide a computationally efficient software implementation of the model. The model has also been studied recently to the satellite-to-ground channel [214] in the context of continuous variable quantum key distribution. While a more complete model of atmospheric propagation for the satellite-to-ground case is described in Vasylyev et al. [218], its much higher complexity makes it unsuitable for a NetSquid embedding.

The beam wandering effects come from two main sources, the turbulence induced beam wandering and the jitter due to the pointing error of the transmitter. The effects of beam wandering due to turbulence depend mostly on the size of the beam at the beginning of the propagation in the atmosphere and are determined by the refractive index structure constant C_n^2 which we will consider as fixed throughout the propagation. The satellite pointing jitter is in turn, characterized by the standard deviation of the pointing error θ_p. The parameters which are necessary to physically describe the channel are the size of the transmitting and receiving stations and the properties of the atmosphere and the pointing system. The main characteristic of the receiving station is the radius of the receiving telescope, that determines the proportion of the transmitted light that can be collected by the receiver.

The current implementation includes two possible configurations for this channel, the ground-to-ground free-space one (class FreeSpaceLossModel) and the satellite-to-ground one (class FixedSatelliteLossModel). The first one considers a horizontal channel, meaning the entirety of the propagation path will happen within the atmosphere and therefore will be affected by it. This can either be the case for communication between two ground stations or for a link between two drones or high altitude balloons carrying telescopes. In both cases, the C_n^2 value is indeed constant and will depend on the altitude of the link. For this configuration, the transmitter will be characterized by the beam waist ω_0.

The second configuration considers a slant propagation path, only the last 10 km of which will be affected by the atmosphere. For this kind of links, a constant C_n^2 is more of an approximation since in reality it varies throughout the propagation path as it is a highly altitude dependent parameter. For this configuration, the transmitter will be characterized by the divergence angle θ_d, a value related to the previously mentioned beam waist as follows: $\theta_d = \lambda/(\pi\omega_0)$.

As for the pointing error of the satellite, assuming that the position of the center of the transmitted beam with respect to the receiving aperture follows a normal distribution and is centered around the midpoint of said aperture, the PDTC will follow a log-negative Weibull distribution. The incidence of turbulence on beam wandering is less important for the satellite-to-ground case, becoming negligible in front of the beam wandering effects due to the pointing error θ_p.

The model assumes that each qubit is affected by the PDTC independently from the other qubits of the transmission. Despite being unrealistic since it neglects the dynamics of the atmosphere, that is considerably slower than the typical time difference between two qubits, it allows to provide a good insight of the average properties of the channel. In addition to this, the satellite-to-ground channel assumes a fixed position for the satellite. This allows to give a first estimate of the performance of the channel when the satellite is on a given position in the sky, but it lacks the ability to provide information about a long-time operation on the channel. We take this into account externally by discretizing the orbit in 10 second intervals for which the satellite is considered as fixed and we then make a separate simulation for each trajectory.

In this work we will use the satellite as a BacQbone node that connects two Quantum cities (see Fig. 6.1). We will suppose that it is able to create and send BB84 states with probability p_{qubit} at a time rate f_{qubit} as well as EPR states with probability p_{EPR} and a rate f_{EPR} to two ground stations.

6.2 Simulation results

6.2.1 Setting and parameters

We will consider the following setting. We suppose that two European Quantum cities, one around the city of Paris with five Qlients and one in the country of Netherlands with three Qlients are realised, allowing metropolitan scale quantum networking. We also suppose that satellites are going over Europe, following an orbit allowing to send photonic states to the Qonnectors (see Fig. 6.2). The Qlients localisation corresponds to actual cities or laboratories. In addition to the Paris Quantum city from the previous chapter, we add a Quantum City in the Netherlands composed of a Qonnector in QuTech at the TU Delft campus and 3 Qlient nodes: Fatou in Amsterdam, Geralt in Den Haag and Hadi in Rotterdam.

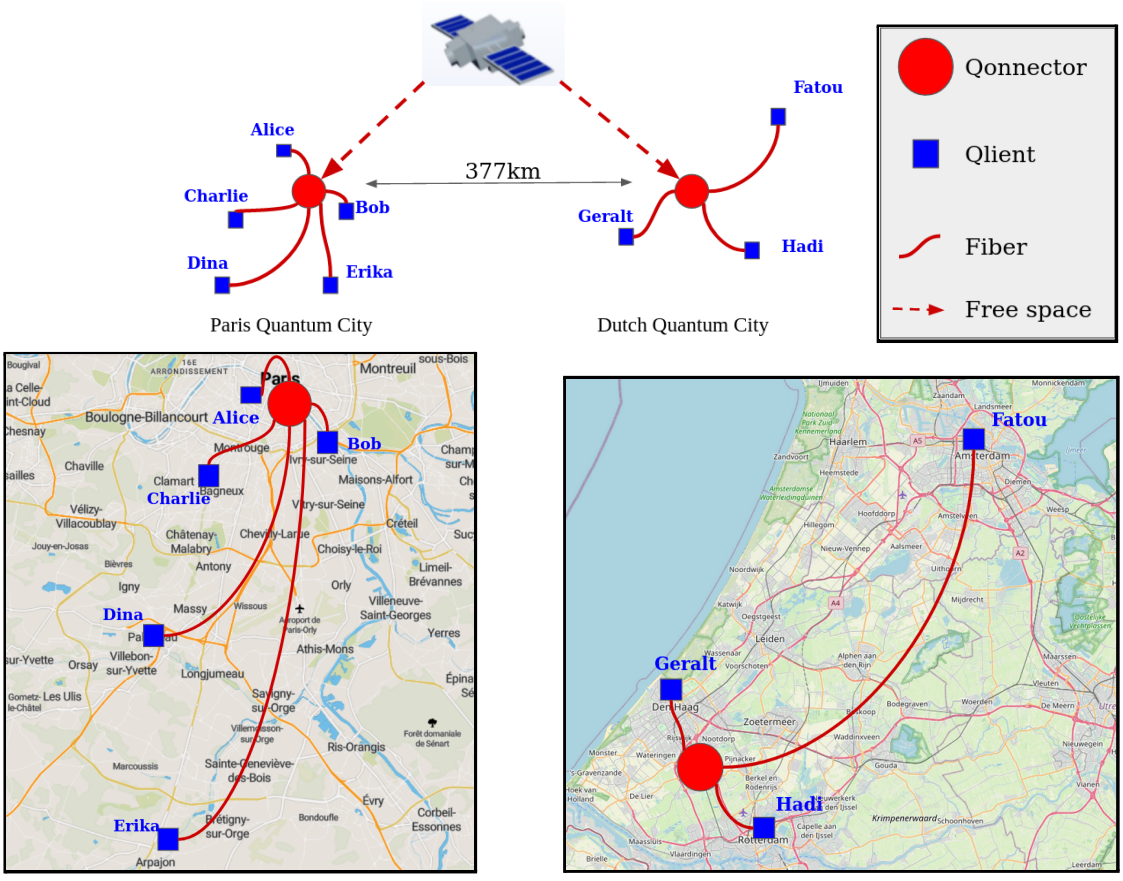


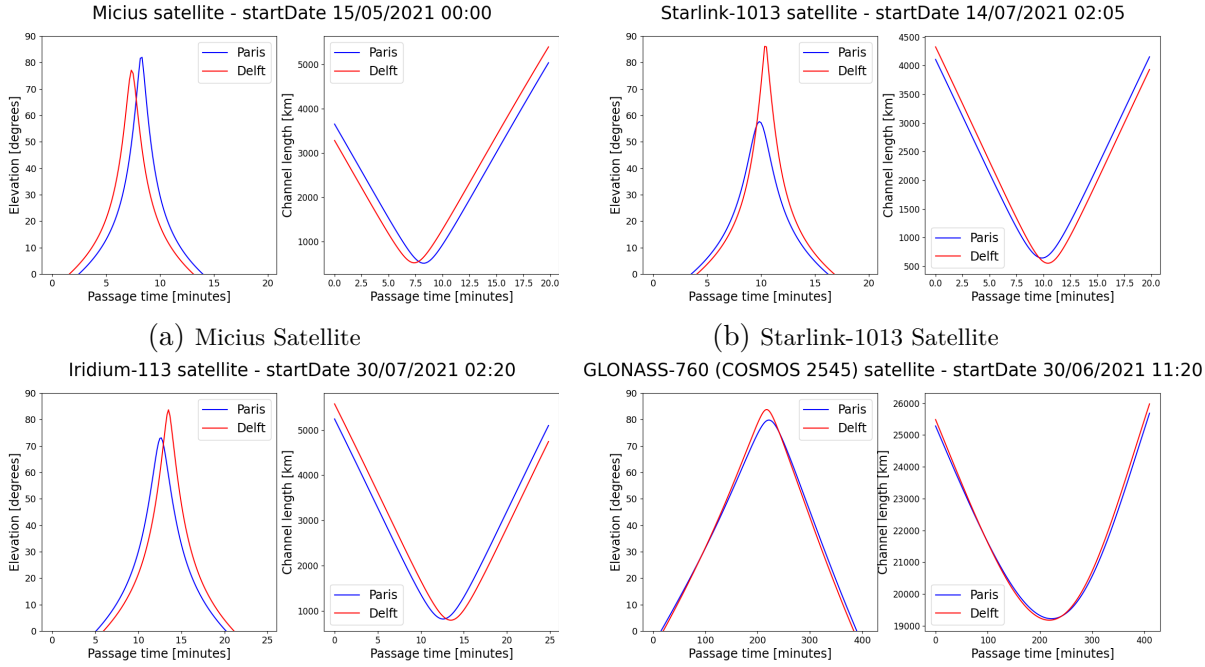
Figure 6.2: A Satellite connecting Paris and Dutch Quantum Cities with downlinks only. Quantum City of Paris: Five Qlients are connected through optical fibers to a Qonnector located in the Sorbonne Université (SU) campus. The length of the fiber links are 1m for the link Alice-Qonnector, 3km for the link Bob-Qonnector, 7km for the link Charlie-Qonnector, 19km for the link Dina-Qonnector and 31km for the link Erika-Qonnector. Dutch Quantum City: Three Qlients connected through optical fibers to a Qonnector placed in Delft. The length of the fiber links are 54km for the link Fatou-Qonnector, 9km for the link Geralt-Qonnector and 13km for the link Hadi-Qonnector.

We recall below the set of parameters used in Chapter 5 to simulate the performance of the Quantum City of Paris. These numbers were extracted from relevant experimental works, including the laboratory in our group.

f_{qubit}	80 MHz	Qubit creation attempt frequency
p_{qubit}	$8 \cdot 10^{-3}$	Success probability of creation of a qubit
p_{flip}	0	Flipping probability at the creation of a qubit
$p_{crosstalk}$	10^{-5}	Probability that the detector flips the outcome
f_{EPR}	80 MHz	EPR pair creation attempt frequency
p_{EPR}	10^{-2}	Success probability of the creation of an EPR pair
p_{BSM}	0.36	probability that a Bell state measurement succeed
$p_{transmit}$	0.81	Probability that transmitting a qubit succeeds
t_{gate}	1 ns	Time it takes to perform an operation on one qubit
$p_{coupling}$	0.81	Fiber coupling efficiency
η_{fiber}	0.18 dB/km	Fiber loss per kilometer
$p_{dephase}$	0.02	Phase flip probability in the fiber
p_{det}	0.95	Detector efficiency (Probability that a measurement succeeds)
R_{dark}	10^2Hz	Dark count rate
Δt_{det}	100 ps	Detector detection gate

We point out that the rate at which single qubit states or EPR pairs are generated highly depends on the source model that we choose, namely Spontaneous-Parametric Down-Conversion (SPDC) in nonlinear crystals that we detail in Sec. 5.2.1. It influences directly the rate at which entanglement can be created between different nodes of our network. This parameter, like all the others, can be tuned freely for each source in our code to match an actual source. For simplicity, we chose in this work to have the same qubit creation rates in Qonnector's source and satellite's source. This is why we focus on the rate, in bit per attempts, at which protocols are performed instead of the throughput in bits per seconds. It gives a less source dependent view on the performance of the communication protocols that we study.

Using real live data from n2yo [219] and the orekit library [220], we are able to find satellites with different orbits and to track down the precise time frame where they would pass over Europe. This also gives us other useful information such as the elevation of the satellite as well as the distance between the satellite and our ground stations at each point in time. In the following we will focus on four different satellite orbits: the QSS (Micius) orbit that was used in [38], the Starlink-1013 orbit, the Iridium-113 orbit and the Cosmos-2545 orbit and we focus on a time frame where the elevation of the satellites allow for quantum communication (usually set at 20 degrees). The first two considered are low Earth orbit (LEO) satellites evolving at around 550km above Earth, with slightly different orbits. The Iridium satellite is higher, around 800km above Earth. Lastly, the Cosmos satellite is a middle Earth orbit (MEO) satellite above Europe, at around 19000km above Earth. In Fig. 6.3 we show the elevation and the distance to the ground stations (Paris and Delft) for these satellites. We point out that our code is modular and that any satellite can be investigated like we do in the following.



(a) Micius Satellite

(b) Starlink-1013 Satellite

(c) Iridium-113 Satellite

(d) Cosmos-2545 Satellite

Figure 6.3: Elevation and distance to Paris and Delft of the Micius, Starlink, Iridium and Cosmo satellites in the time frame considered.

6.2.2 Simple down link scenario: Choosing a satellite

To test our model, we first simulate a simple down link scenario between each of the satellites and the Qonnector from Paris. This will allow us to choose the satellite that is most suited for quantum communications.

The down link scenario simulation goes as follows: for each point in the orbit where the satellite's elevation is over 20 degrees, the satellite starts sending BB84 states to the Qonnector in Paris for one second while recording the time stamp of each state. The Qonnector receives, measures the states and records the measurement outputs. We can thus estimate the rate, i.e. the number of states received over the number of states sent, which also corresponds to the link efficiency at this point in the orbit. We average this over ten runs to get a better estimate. After this is done we move on to the next point in the orbit, ten seconds later. We show the result in Fig. 6.4 and in Table 6.1 for a given set of parameters.

Satellite	Maximum rate
Micius	0.238
Starlink	0.157
Iridium	0.101
Cosmo	0

Table 6.1: Maximum rate for the four satellites. The maximum rate is the rate, i.e. the number of qubits received at the ground station over the number of qubits sent from the satellite, when the satellite is closer to the ground station.

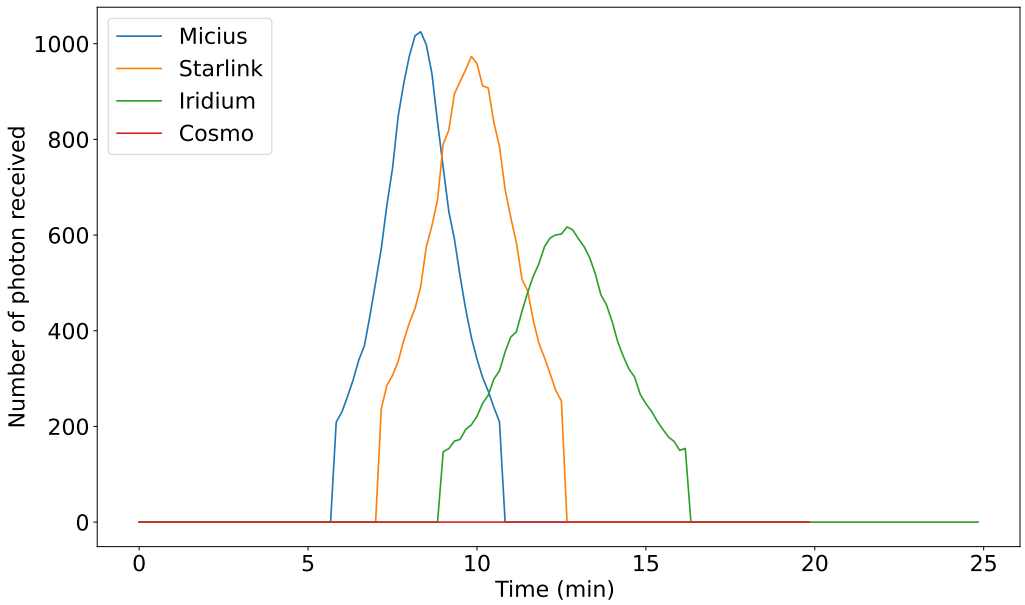


Figure 6.4: Comparison of the average number of photons received in Paris for the four satellites considered for approximately 6000 photons sent by the satellite at each point of its orbit. For this simulation we suppose there are no aerosols in the atmosphere and we set the aperture radius of the receiving telescope at 1m, the beam divergence at 5e-6 radians and the pointing error at 5e-7 radians.

As expected, distance and elevation of the satellite impact the number of states that arrive at the ground station. For example, we can see that none of the photons sent by the Cosmo satellite arrives at the Earth. MEO satellites, while having the advantage of having a longer time frame in which the elevation allows for quantum communication, are too far for single photon states to arrive at a precise point on Earth. It follows that geocentric satellites at a height of 36000km above ground, while having the advantage of always being visible by a given ground station, would, under typical conditions, be too far for the photons to arrive at the ground stations. As it is located further than the other two satellites, the Iridium satellite has a lower rate but a longer exploitation time. We thus identify the well-known trade-off in satellite communication between distance of the satellite to the Earth and time frame in which we can use it. Micius and Starlink satellites are performing better but as can be seen in Fig.6.3b, the elevation angle of Starlink with respect to the Paris ground station is lower than the one of Micius. This means Starlink does not pass exactly above Paris which causes a drop in the rate.

6.2.3 Influence of the parameters

As detailed in Sec. 6.1, our loss model allows us to analyse the effect of a few parameters of satellite communication, namely the aperture radius of the receiving telescope, the beam divergence, the pointing error and the the aerosol model, which affects directly the atmospheric transmittance. In this section we study the effect of these different parameters on the rate of the down link scenario. We chose to focus on the Micius satellite for the rest of this section as it exhibits the best performances with the Paris node. When studying the influence of a parameter, we fix the other ones to what we expect to be the best value achievable in the near future: an aperture radius of the receiving telescope of 1m, a beam divergence at 5×10^{-6} radians and a pointing error at 5×10^{-7} radians. We also suppose that the effect of the atmospheric turbulence are negligible with respect to the parameters studied.

We start with a study of the atmospheric model. In Sec. 6.1 we have detailed a few atmospheric models that have an effect on photonic communication in free-space. Here we will study the ideal case where there is no aerosol between the ground station and the satellite, the rural5 and rural23 models that correspond to ground stations in rural areas with a meteorological range of, respectively, 5 and 23 km, the urban5 model that correspond to a ground station close to a city and the navy model corresponding to a ground station in the middle of the sea. Meteorological range is usually defined as the length of atmosphere over which a beam of light travels before its luminous flux is reduced to 5% of its original value. In Fig. 6.5 we show the number of photons received at the ground station in Paris when considering these different atmospheric models. This simulation has been done as the one in the previous section, meaning that BB84 states are sent by the satellite for each point of the orbit where the elevation of the satellite is over 20degrees.

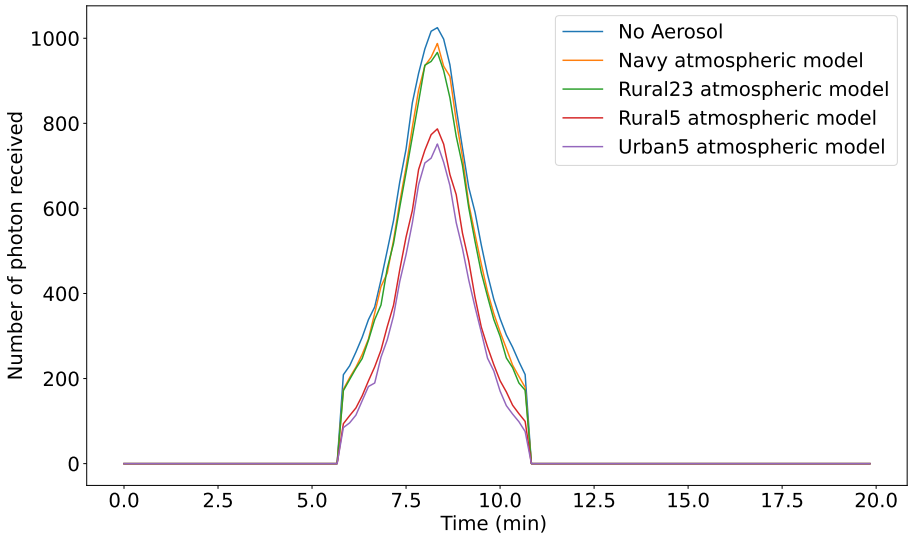


Figure 6.5: Effect of different aerosol models on the number of photonic qubits arriving from the Micius satellite.

We then study, using again the down link scenario, the effect of modifying the other parameters included in our model. This study allows us to know what to expect from a specific setting and to identify the key parameters to improve future quantum communication. We choose values that are considered as realisable with current or near term technology.

We see that the transmitter parameters do not have all the same importance. A change of 5 micro-radians in the beam divergence angle (see Fig. 6.6), has a drastic effect on the number of photons arriving at the ground station. On the other hand the pointing error of the transmitter (see Fig. 6.7) has to be multiplied by five in order to reduce the number of arriving photons by a half. Finally, we see that increasing the aperture radius of the receiving telescope at the ground station by 20cm can almost double the number of qubits successfully measured (see Fig. 6.8). This last parameter can be the easiest to improve in future experimental realizations.

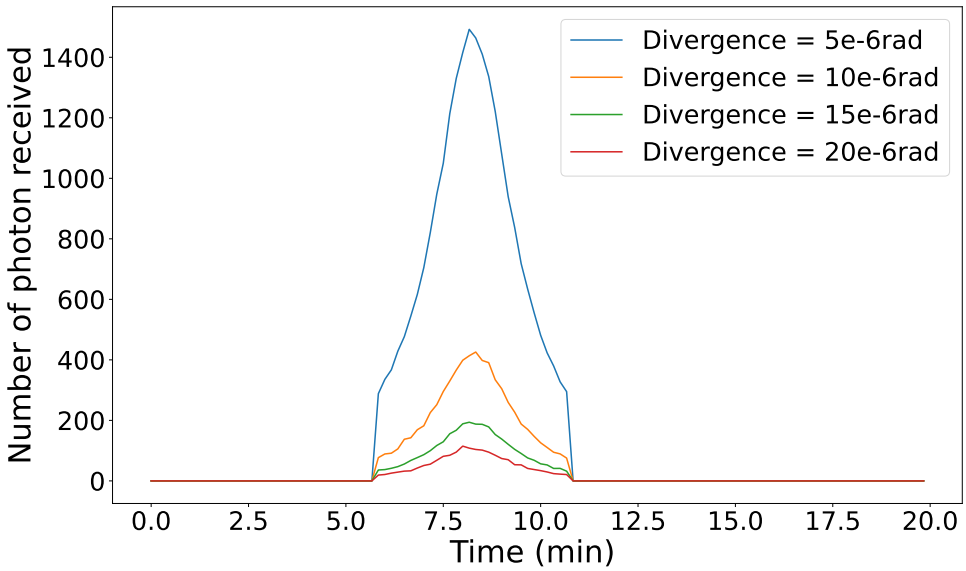


Figure 6.6: Effect of the beam divergence angle θ_d on the number of photonic qubits arriving from the Micius satellite.

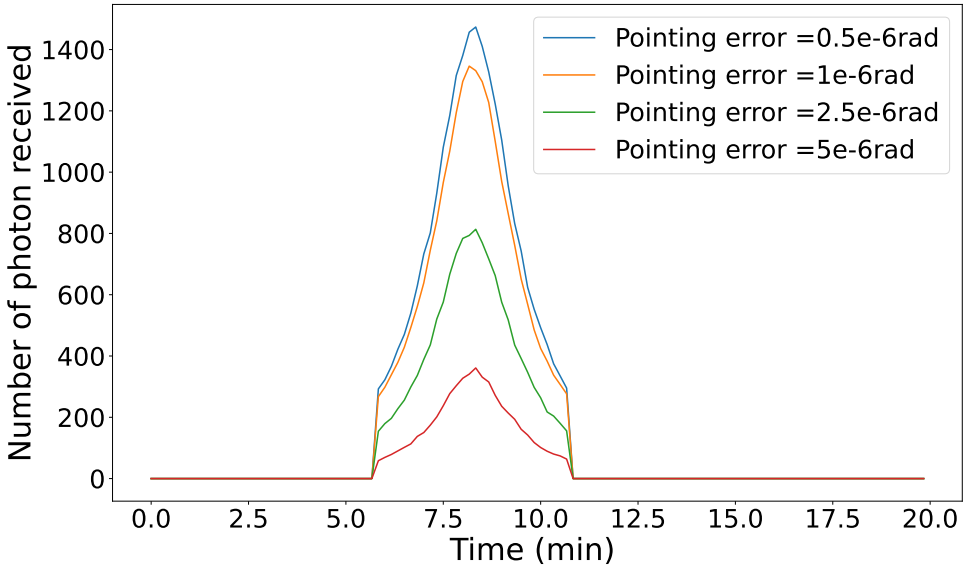


Figure 6.7: Effect of the pointing error θ_p on the number of photonic qubits arriving from the Micius satellite..

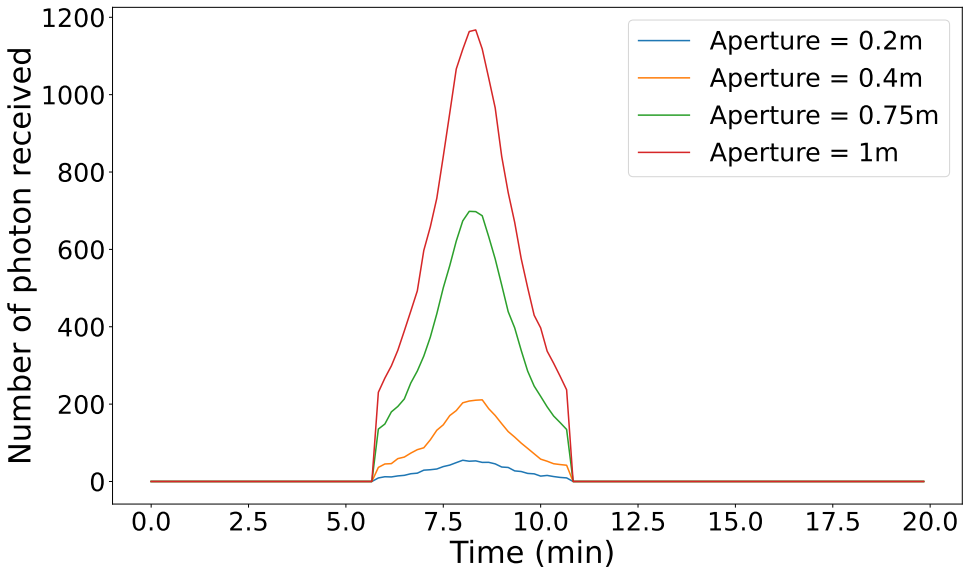


Figure 6.8: Effect of the aperture radius of the receiving telescope R_x on the number of photonic qubits arriving from the Micius satellite.

6.3 Quantum Key Distribution between two Qlients.

In this section we reconnect with the path to quantum Internet and show the performance of satellite communication in the context of linking two Quantum Cities. We study the achievable QKD rate between two Qlients respectively from the quantum city of Paris and the Dutch quantum city connected via the Micius satellite (see Fig. 6.2 and 6.3a). We will consider the most optimistic set of parameters from the previous section, namely no atmospheric turbulence, an aperture radius of the receiving telescope of 1m, a beam divergence at 5×10^{-6} radians and a pointing error at 5×10^{-7} radians.

Let us imagine that one Qlient from the Paris Quantum City, say Bob, wants to generate a secret key with a Qlient from the Dutch Quantum City, say Hadi, using a QKD protocol. There are different protocols achieving this functionality and we focus our analysis on two of them. For a more extensive study of the different ways of achieving QKD in a metropolitan network, see Chapter 5. In the following we show the feasibility of two QKD scenarios, one trusted and one untrusted, and then we discuss how realistic they actually are.

6.3.1 Trusted satellite

The most natural way to achieve key distribution between Bob and Hadi is to perform BB84 between all the nodes between these nodes while trusting each of them not to reveal the key. More precisely the satellite performs two BB84 protocols in parallel to establish two keys with the Qonnectors from the two cities, k_{Paris} and k_{Delft}. At the same time the two Qlients establish secret keys, k_{Bob} and k_{Hadi} using the BB84 protocol with their Qonnector. Once all keys are created, the Parisian Qonnector can send k_{Bob} to the satellite using k_{Paris}, the satellite forwards it to Delft's Qonnector using k_{Delft} who sends it to Hadi using k_{Hadi}. In the end, Bob and Hadi share k_{Bob}.

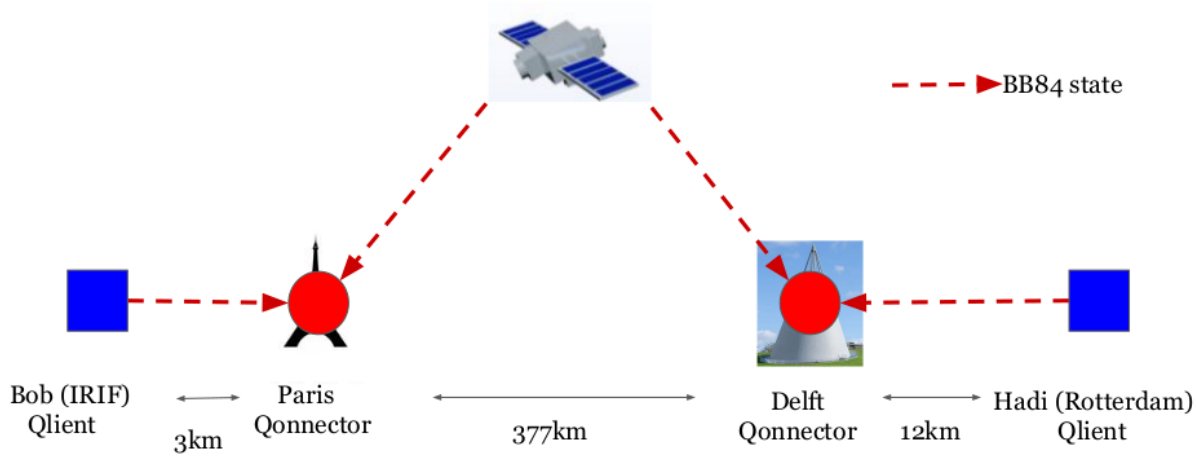


Figure 6.9: QKD between Bob and Hadi: All trusted node Scenario. Here the satellite performs two BB84 protocols in parallel to establish two keys with the Qonnectors, k_{Paris} and k_{Delft}. At the same time the two Qlient establish secret keys, k_{Bob} and k_{Hadi} using the BB84 protocol with their Qonnector. Once all keys are created, the Parisian Qonnector can send k_{Bob} to the satellite using k_{Paris}, the satellite forwards it to Delft's Qonnector using k_{Delft} who sends it to Hadi using k_{Hadi}. In the end, Bob and Hadi share k_{Bob}

As in the previous section we simulate the sending of BB84 states to both ground stations and get the rate for the two satellite to ground links. We also simulate the sending of BB84 states from each Qlient to the Qonnectors. A more extended study of the different ways to perform BB84 in the Quantum City of Paris can be found in Chapter 5, from which we extract some of the simulation results. We also simulate the sending of BB84 states from each Qlient of the Dutch Quantum City to their Qonnector. The parameters for the hardware at each node are listed in Sec. 6.2.1. We show the results of these simulations in Fig. 6.10 and Table 6.2.

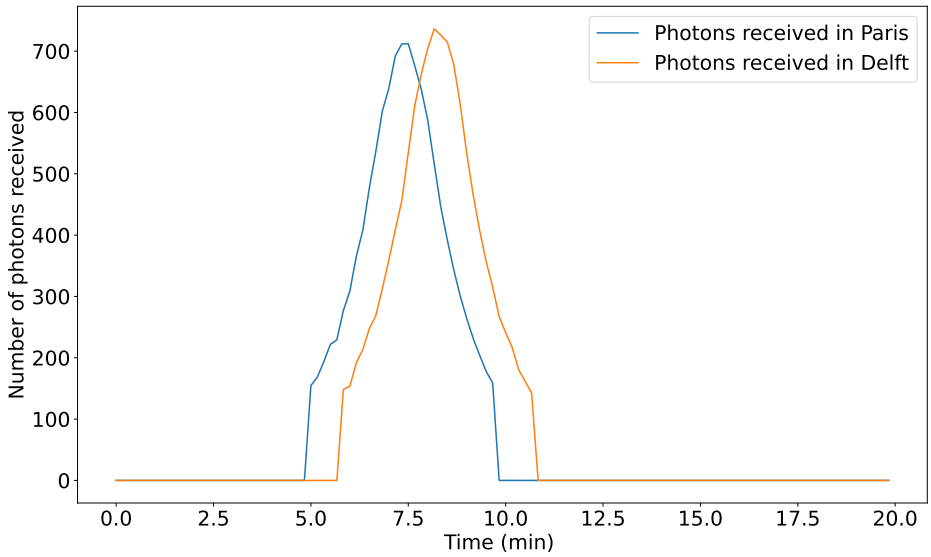


Figure 6.10: Average number of photons received in Paris and Delft for approximately 3000 photons sent from the satellite at each orbit point.

Nodes involved	Rate (sifted key bit per channel use)
Satellite − >Paris Qonn	0.238
Satellite − > Dutch Qonn	0.228
Alice − > Paris Qonn	0.423
Bob − > Paris Qonn	0.374
Charlie − > Paris Qonn	0.322
Dina − > Paris Qonn	0.180
Erika − > Paris Qonn	0.115
Fatou − > Dutch Qonn	0.043
Geralt − > Dutch Qonn	0.296
Hadi − > Dutch Qonn	0.253

Table 6.2: Performance of the BB84 protocol between all nodes. The first two lines correspond to the Satellite sending BB84 states to the two ground stations, and the other lines correspond to BB84 rate with each Qlient of the two Quantum Cities.

As expected, the longer a photon has to travel in a fiber the lower is the rate. In this scenario, the rate of the overall key distribution protocol is given by the minimum rate of each sublink. Hence depending on the pair of nodes that want to establish a secure key, the limiting sublink can be the satellite-to-ground link or the fiber link inside the Quantum City. For example if Hadi and Bob want to perform this trusted-node QKD protocol, their total rate is limited by the rate of the satellite to ground link. But if Erika and Fatou want to do the same, it is the fiber link between Fatou and her Qonnector that is most limiting. Note that the satellite-to-ground rate here is the rate when the satellite is at its optimal position, namely just above the ground stations. As an example with a source rate of 80 MHz, the raw key throughput at this point of the orbit 1.7Mbit/s for Bob and Hadi and 300kbit/s for Erika and Fatou. We discuss how realistic this value is in Sec. 6.3.3. Note also that in order for this scenario to securely create a key between two Qlients, all the nodes (Qonnectors and satellite) along the path between two Qlients have to be trusted.

6.3.2 Untrusted satellite

Another way to distribute a key between Hadi and Bob is to use the entanglement-based version of QKD also known as Ekert protocol or, in its simplest version, BBM92 (see Sec. 2.1.1.2 for a detailed explanation of the protocol). The goal here is to have an EPR pair shared between our two Qlients. Once this is done, by simply measuring their qubits in random bases and sifting the outcome, Hadi and Bob get a correlated list of bits. They can then use a part of this list to check that no one attempted to corrupt their quantum communication and use privacy amplification techniques to transform the remaining part of the key into a shared private key.

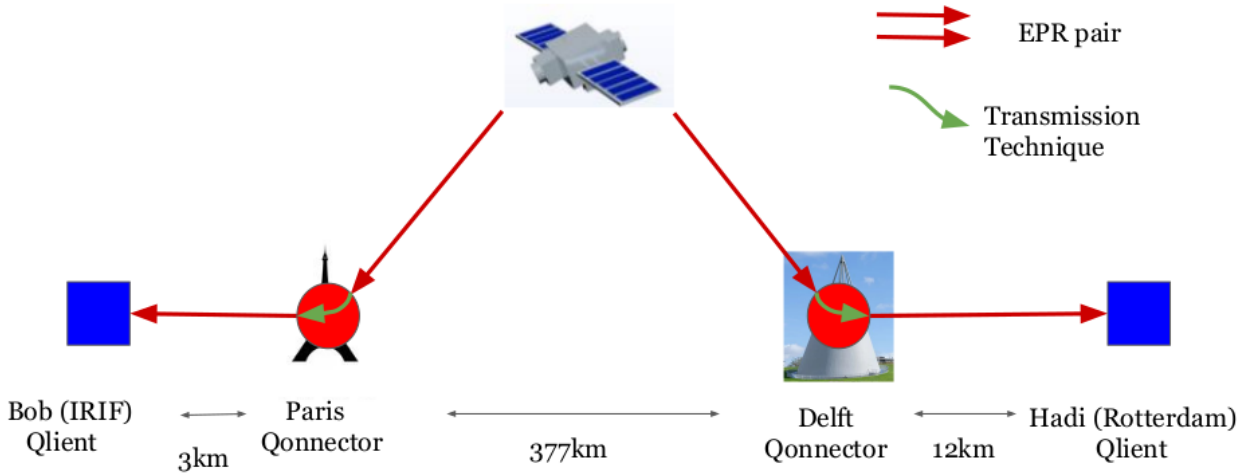


Figure 6.11: QKD between Bob and Hadi: Untrusted nodes. Here the satellite performs the BBM92 protocol directly with the Qlients. The Qonnectors are used as transmitting stations, that couple the photons arriving from the satellite into a fiber and send them to the Qlients.

In the context of Quantum Cities connected by a satellite, the protocol goes as follows (see Fig. 6.11): an EPR pair in the state $|\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$ is created at the satellite and each qubit of the pair is sent to two Qonnectors at the ground. Once there, it is coupled into an optical fiber and transmitted to each Qlient who measures it. They then keep the outcomes that had been measured with the same timestamp to post-select the qubits that came from the same pair. These steps are performed for each point of the Micius orbit where the satellite's elevation is above 20degrees for both Qonnectors. The coupling of a photon coming from a satellite into a fiber succeeds with probability $p_{transmit}$ that we fix to 81% here as it is the theoretical maximum [221]. Coupling photons arriving from a satellite into a fiber is done through adaptive optics to correct the effect of the atmosphere. The optimization of this process is currently investigated by the research community [222]. This parameter is of course freely tunable in our simulation.

After simulating the process described above for each point in the satellite orbit and averaging over tens of run, we can have an estimate of the rate by simply looking at the ratio between the number of pairs sent from the satellite and the number of pairs received by the Qlients. We show results of simulations with different pairs of Qlients in Fig. 6.12 and Table 6.3.

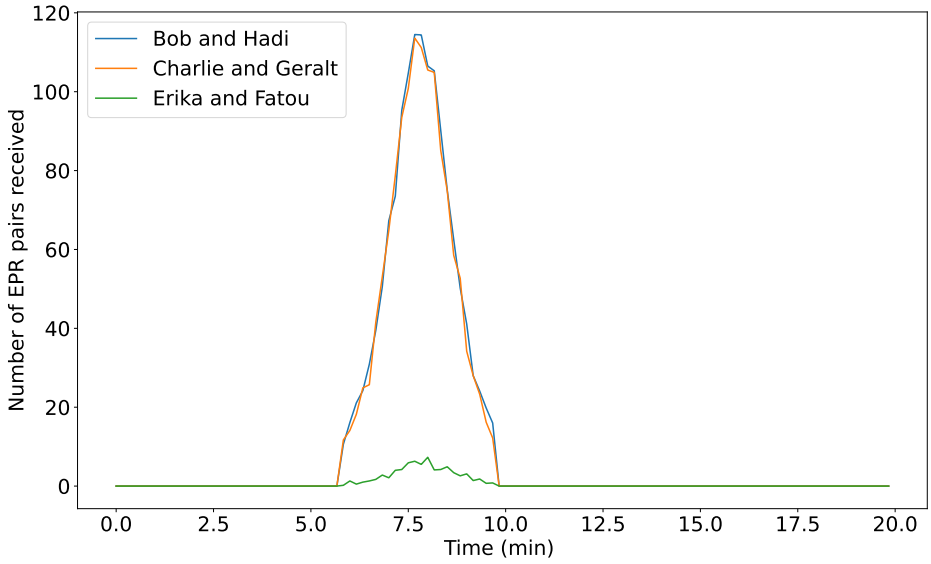


Figure 6.12: Average number of successful EPR pair transmissions from the Micius satellite to pairs of Qlients in the two Quantum Cities considered. For each point of the orbit we simulate the sending of approximately 650 EPR pairs from the satellite and average over 10 rounds.

Qlient pairs	Maximum rate
Bob & Hadi	0.0183
Charlie & Geralt	0.0185
Erika & Fatou	0.0019

Table 6.3: Average maximum rate for pairs of Qlients of the two Quantum Cities considered.

Here, in addition to the loss due to atmosphere between the satellite and the ground stations, the rate

is affected by the distance photons have to travel in optical fibres from the Qonnectors to each Qlient. As expected the longer this distance is, e.g. for Erika and Fatou, the lower the rate is. This is also why the rate is similar for the two pairs of Qlient Bob & Hadi and Charlie & Geralt: the distance photons have to travel into fibers is comparable (see Fig. 6.2). With a source rate of 80 MHz, the raw key throughput would be 150kbit/second for Hadi and Bob, and 14kbit/second for Erika and Fatou. This scenario has a lower rate than the one presented above but presents a non-negligible advantage: Qonnector nodes and satellite do not have to be trusted. Indeed the Qlients can check if their communication was disturbed by using part of their measurement outcomes. This trade-off between time and security is found in almost all communication protocols.

6.3.3 Realistic quantum key distribution

The above simulations illustrate the feasibility of quantum key distribution between two quantum cities separated by a few hundreds of kilometers. However this analysis assumes that the satellite is always at its optimal point in its orbit. This is clearly unrealistic since, as we saw in Sec. 6.1, the time span in which a satellite's elevation allows for quantum communication is only five to ten minutes. The QKD rate significantly drops when we take this into account. For example in the trusted scenario above, the total raw key established between the Micius satellite and the Paris ground station during the whole passage of the satellite above Europe is of length 17kbits on average. This limits drastically the amount of messages that can be securely sent between the two Qlients considered.

A few solutions arise to get more useful key distribution rates. The first is to use multiple passages of a satellite over several days to create and store keys at the ground stations. These keys can be established using one of the two scenarios presented. They can later be used to establish a secure communication channel between the Qlients. This is useful in a scenario where different quantum cities need to communicate securely only for a few specific applications. It can be envisioned, for example, in the context of governmental communications, or for some targeted business communications. One possible downside of this solution is that the keys have to remain secure at the Qonnector nodes until they are used, which could be a week away from the day they were established. Security of the facilities have to be ensured during this time. It might seem limiting at first, however, in the near term, there will probably be very few applications that really need the information-theoretic security that QKD offers. Post-quantum communication protocols are expected to ensure the security of classical communication even when quantum computers start to appear.

Another solution is to use a constellation of satellites orbiting around the Earth. The idea is simple: once a satellite is out of reach for quantum communication, we wait for the next one to start creating key. In this case, finding the optimal orbit height and the optimal number of satellites on this orbit is a complex question that we leave for further work. We refer the reader to [223] for a more detailed study of this problem.

Some other issues have not been taken into account in this study that might reduce the final QKD rate. For example in this section, we neglected atmospheric turbulences that may vary with the position of the Qonnector and the timing of the experiment. Satellite quantum communication is very dependent

on the pollution and weather conditions at the time of the key establishment. Moreover in our simulations we supposed the wavelength of the photon to be 1550nm which is convenient for coupling them with telecom equipment at the ground. In the Micius experiment however [38], the wavelength considered is 850nm and would have to be converted to telecom wavelength to be included in our network model. This would induce more loss in the second scenario that we considered above.

We hope this study shows the possibilities and limitations of satellite communication to link local networks. According to our simulations, current technologies could already allow for interesting applications between distant cities, as we will show in the next section.

6.4 Discussion

6.4.1 Comparison with ground-based communication

As we mentioned in the introduction, current quantum repeater technologies do not allow for positive QKD key rates over the distances that we consider here. Since the distance between the Dutch Quantum City and the one of Paris is 377km, according to the study from Chapter 4, we would need five to ten repeaters to divide the link into sublinks of sufficiently small length. However the noise induced by the repeater operations in each sublink is still too high for giving any kind of communication advantage [209, 208] unless considering boosted performances [202]. Reasons for this depend highly on the repeater model that we consider. Overall the repeater parameters could be separated into two categories: the ones affecting the time it takes to generate entanglement in a sublink (e.g. probability of emission, of coupling into fibers, of detection) and the ones affecting the swapping operation in middle nodes (e.g. Bell state measurement success probability, two qubits gates noise). Many proposals to overcome these issues are under investigation such as the use of multiplexing [224, 225] or all photonic quantum repeaters [24].

Another solution that could be envisioned is the use of drones or high-altitude balloons. Let us imagine a key distribution scenario using two stationary high-altitude balloons 10km above the Paris and Dutch Qonnectors. One trusted-node QKD scenario is to build a path between the two Qlients, as we show in Fig. 6.13, and to perform the BB84 protocol between each node. As in Sec. 6.3.1, the protocol used to have a shared key between the two Qlients consists in establishing secret keys between each node along the path and then to use these keys to transmit a key from one Qlient to the other. The final rate is thus given by the minimum of the rate of every sublink along the path.

Using the free-space loss model described in Sec. 6.1 we can make a rough estimate of the QKD rate between the two balloons and between each balloon and the Qonnector below. To get a estimation, we suppose that the aperture radius of the receiving telescope in the balloons is 40cm, we fix the beam divergence at 5×10^{-6} radians and the pointing error at 5×10^{-7} radians. We compute separately the horizontal atmospheric transmittance between the two balloons (around 0.96) and the vertical atmospheric transmittance between the balloon and the ground (around 0.9). As the free-space communication happens in the atmosphere, we can no longer neglect the effect of the refractive index structure constant C_n^2. The value of C_n^2 depends on the height of the high-altitude balloons. As we show in Table 6.4, this value has a drastic effect on the communication rate between the two balloons.

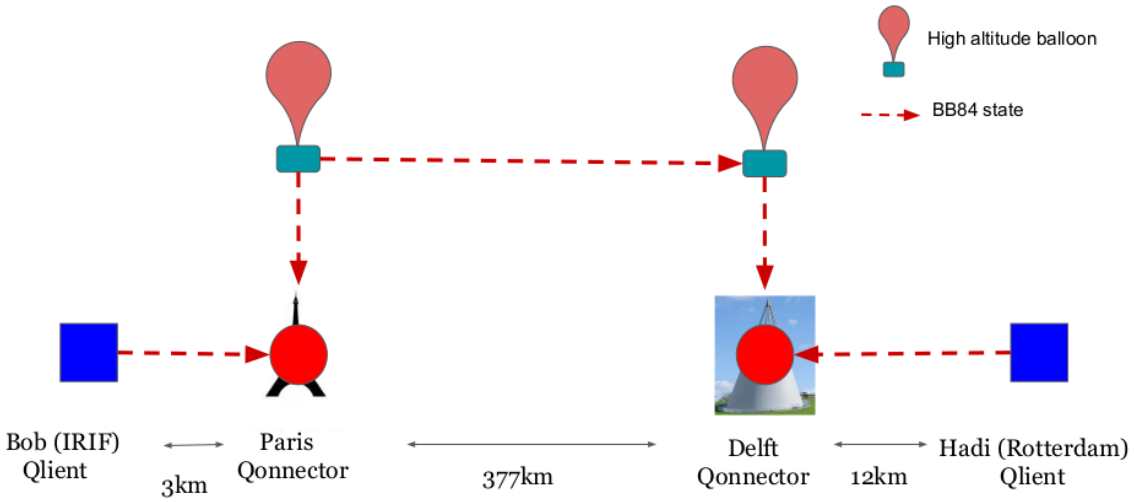


Figure 6.13: A trusted node QKD scenario between two Qlients using two high-altitude balloons over the Qonnectors. We suppose that the drones are 10km above each Qonnector.

Value of C_n^2	Rate
0	0.138
10e-18	0.079
10e-17	0.014
10e-16	0.001
10e-14	1e-5

Table 6.4: BB84 rate for balloon-to-balloon communication for different values of C_n^2. The balloons are separated by 377km.

In what follows we chose an optimistic yet non-zero value for C_n^2 between the two balloons, namely 10e-18. For the balloon-to-Qonnector links we fix C_n^2 at 10e-16 and take the aperture radius of the receiving telescope at the Qonnector to be 1m. In Table 6.5 we show the rate for all the sublinks between Bob and Hadi.

Sublink	Rate
Bob $->$ Paris Qonn	0.374
Paris Drone $->$ Paris Qonn	0.463
Paris Drone $->$ Dutch Drone	0.079
Dutch Drone $->$ Dutch Qonn	0.463
Dutch Qonn $->$ Hadi	0.253

Table 6.5: BB84 rate for every sublink across the path between Bob and Hadi

Note that this gives us only a first estimate of the BB84 rate between two Qlients in Quantum Cities linked with high altitude balloons. It however shows the feasibility of such free-space links, which could come as a handy solution to perform quantum communication when satellites are not available. Theoretically, two balloons at 10km altitude can be separated by a maximum 714km and still be visible in the horizon. We leave a more detailed study of these kind of high-altitude balloons links for future works.

6.4.2 Towards quantum Internet applications

Once entanglement is generated between the Qonnectors of our two Quantum cities, a new range of applications becomes available to the Qlients. As we detailed in Chapter 2, there are a few multipartite applications based on first the sharing of a GHZ state $\frac{|0\rangle^{\otimes n}+|1\rangle^{\otimes n}}{\sqrt{2}}$ [5] to all the Qlients and then measuring and processing the outcome. For example some conference key agreement protocols [88, 87], the multipartite counterpart of QKD allowing n parties to get a secure shared key are based on such techniques. Anonymous transmission [93] or electronic voting [101] are also examples of protocols taking advantage of correlations obtained through GHZ state measurements. Through Bell state measurements and local corrections, two GHZ states and a Bell pair can be transformed into a bigger graph state suitable for these applications as we show in Fig. 6.14. For more information about graph state manipulation, see e.g.[30, 29].

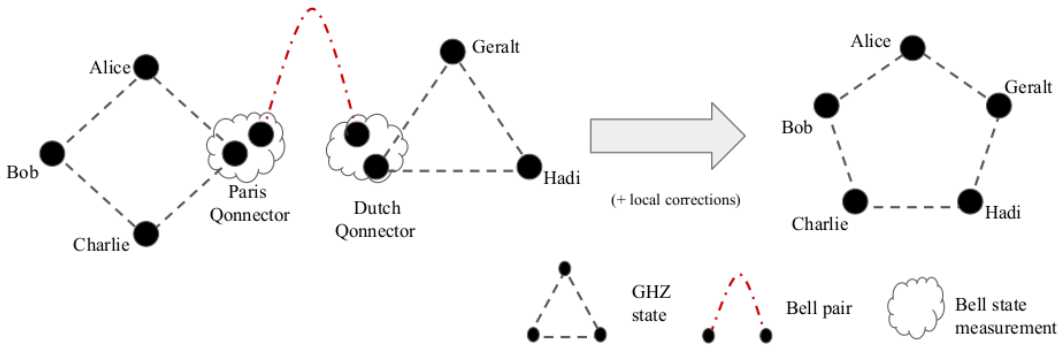


Figure 6.14: By making Bell state measurements and local corrections, two GHZ states generated in Paris and the Netherlands can be transformed into one single shared GHZ state, consuming one Bell pair.

The main obstacle to performing these protocols is precisely the sharing of these multipartite entangled states. As we detailed in Chapter 3, security properties often rely on performing many rounds of GHZ state verification to ensure that nobody is altering the protocol. This means that our network should be able to efficiently create and share thousands such states in a relatively short time. Unfortunately this is unrealistic with current hardware performances. As explained in detail in Chapter 5, photonic GHZ states are created by simultaneously creating Bell pairs that are then entangled using fusion gates [205]. All these processes are probabilistic and this makes the probability of succeeding in creating a GHZ state very low: on the order of 10^{-3} for 3 or 4 qubits GHZ states and 10^{-5} for 5 or 6 qubits GHZ state.

While technologically out of reach for now, these applications are theoretically possible in our Qloud architecture. It is crucial to think ahead on how future network applications will be performed when designing near-term quantum networks. This will avoid energy waste on constructing architectures that have to change with new applications. The Qloud architecture is also convenient for a new user to join as it only has to connect to one Qonnector of a Quantum City. Future work will explore how communication between bacQbone nodes could be optimized to facilitate communication of two Qlients in distant Quantum Cities, for example Dina and Alice in Fig 6.1.

6.5 Conclusion

In this Chapter, we have studied the feasibility of satellite quantum communication between two Quantum Cities in Europe using simulation results from a library based on the Netsquid network simulator. This method allowed us to try out different scenarios without actually using satellite and gave us the freedom to test different hardware parameters. We showed performances of different QKD scenarios in a specific realistic setting. This motivates the building of the Qloud architecture of Fig 6.1 as it minimizes end user hardware while facilitating routing of entanglement. We also discussed alternatives to satellite communication for connecting different Quantum Cities, such as high-altitude balloons.

All of these results are promising and show that the Quantum Internet is not a dream for the far future anymore, but something that engineers could already start constructing. Alternatives to fiber-based communication, e.g. a hybrid combination of satellite constellations and high-altitude antennas, could be the missing link to enable long-distance communications. There are however both experimental and theoretical issues to deal with before putting in the money and energy to actually send satellites around the Earth. The limited exploitation time of satellites actually questions the suitability of satellite-based quantum communications. There is, for now, a lack of realistic strategies to get longer exploitation times. The research community should focus on precise use cases and analyze whether the effort of creating satellite links is actually worth it.

Conclusion and Outlook

In this thesis we have explored different aspects of the development of a global quantum network that we could call the quantum Internet. We first introduced some definitions and network consideration to help with the understanding of the rest of the work. We showed the current goals set by the international quantum Internet research community and challenges that arise in front of us. We also introduced some of the protocols that will push the boundaries of today's web capabilities. Without being exhaustive, we hope this gives a glimpse of the future revolution that quantum information will bring to communication networks.

We then have discussed composable security properties of a specific building block network protocol called multipartite entanglement protocol. As it is used as a building block in many multipartite protocols, it is crucial to be able to perform it many times sequentially without security breaches. We have showed composable security of this protocol against a possibly malicious source and have discussed some issues of the current framework used to prove composable security. As a follow-up, we will explore in the near future a more general verification protocol for any graph state with an updated framework.

After that, we have showed the limitation of current hardware in the establishment of quantum repeater protocols that would allow long distance communication between two nodes. We studied and modeled a specific hardware choice for local nodes, the NV center. We analyzed the effect of imposing a cut-off, a maximal number of entanglement establishment attempts on a sublink before moving on to the next one. We showed that current capabilities, especially in photon generation rates and coherence time of NV centers, limit greatly the distance at which bipartite entanglement can be created. A natural follow-up to this work is to explore other hardware in the same way. We also hope this gives experimentalists some kind of a roadmap to which parameters they should try to improve.

We then introduced our vision for a quantum Internet architecture that would both be scalable and minimize end users hardware. It starts with a model for metropolitan quantum network that we call the Quantum city. After a precise modeling work of what we can achieve today or in the near term in Sorbonne Université's laboratories, we have simulated the performances of bipartite and multipartite applications in a Parisian instance of a Quantum City. We tried to highlight the important hardware parameters and to link them to actual implementation of useful network protocols. We notably showed that the generation rate of multipartite entangled states such as the GHZ state is for now limiting multipartite network applications. The outlook here consists in expanding in more detail how the central node of this architecture, the Qonnector, would actually perform its operations. A more detailed study

of the timing at which local operations are performed would be crucial too, as we mostly neglected this during this study. It would also be interesting to look at what new applications could be available should some end user nodes hardware improve with for example quantum memories.

We finally modeled satellite and balloon communication to scale up local networks to continental and transcontinental networks. We have studied different bipartite scenarios to establish secret key between two users from distant Quantum Cities, using real satellite data. We have tried to highlight the important parameters and issues to resolve in order to establish large-scale quantum networks and perform useful applications. In particular we highlight the issue of establishing long-distance links that would be available all the time. The time frame in which satellites are available for quantum communication is very small and we discussed some solutions to this problem such as using balloon-based free space links. A natural follow-up to this work would be to explore other solutions and strategies to establish long-distance quantum communication links, with different hardware such as satellite constellations.

A large part of the results given in this thesis were obtained using a library of functions that we constructed on top of the NetSquid network simulator. We used this library to model protocols on specific quantum network instances including as much hardware parameters as possible. One contribution of this work thus is this network simulator, that can be found on GitHub and that we document in Appendix B. We hope to continue improving this simulator for future NetSquid users.

My personal outlook is to study yet another aspect of quantum communications which seems crucial for near term development, namely the energy consumption of such networks. We hope in the near future to develop a framework for studying how much energy is consumed by a specific protocol using a specific hardware. We also hope to understand how the energy consumption scales with the parameters of the protocol such as the number of parties involved or the length of the message to transmit. This might rule out some of the hardware or strategies that we now have in mind for network protocols. This kind of study seems essential to avoid a waste of time and resources.

We hope that the work done in this thesis shows that the quantum Internet is not a dream for the far future. Many efforts are congregating to perform the first useful quantum network protocols. As we said in the introduction, it is still hard to grasp where this will lead us but there is no doubt that it will have tremendous implications on our daily lives.

APPENDIX A

Appendices for Chapter 4

A.1 Losses and noise on the photonic qubits

In this Appendix we describe how the losses and noise affect our photonic qubits. In particular, we first recall how the two types of encoding result in the losses acting as different quantum channels on the states. Then, we study the effects of a finite detector time-window. More specifically, we firstly show that the arrival of a photon outside the time-window is equivalent to all the other loss processes and secondly we calculate the probability of registering a dark count within the time-window. We also show how to model the noise arising from those dark counts for the SiSQuaRe and SPADS schemes. Finally, we calculate the dephasing induced by the unknown phase shift for the single-photon scheme.

Effects of losses for the different encodings

The physical process of probabilistically losing photons corresponds to different quantum channels depending on the qubit encoding. In our repeater schemes we use two types of encoding: time-bin and presence-absence of a photon. For a time-bin encoded qubit in the ideal scenario of no loss we always expect to obtain a click in one of the detectors. Hence loss of a photon resulting in a no-click event raises an erasure flag which carries the failure information. Therefore it is clear that for this encoding the physical photon loss process corresponds to an erasure channel with the erasure probability given by one minus the corresponding transmissivity,

$$D(\rho) = \eta\rho + (1-\eta)\,|\perp\rangle\langle\perp| \ . \tag{A.1}$$

Here $|\perp\rangle$ is the loss flag, corresponding to the non-detection of a photon. Since we are only interested in the quantum state of the system for the successful events when a detection event has occurred, we effectively post-select on the non-erasure events. For presence-absence encoding the situation is different since now there is no flag available that could explicitly tell us whether a photon got lost or not. In fact for this encoding the photon loss results in an amplitude-damping channel applied to the photonic qubit. Here the damping parameter equals one minus the transmissivity of the channel [226].

Effects of the detector time-window

The detector only registers clicks that fall within a certain time-window. It is *a priori* not clear what kind of noisy or lossy channel should be used to model the loss of information due to non-detection of photons arriving outside of the time-window. This is because in a typical loss process we have a probabilistic leakage of information to the environment. In the scenario considered here, the situation is slightly different as effectively no leakage occurs, but rather certain part of the incoming signal effectively gets discarded. Here we will show that despite this qualitative difference, within our model this process can effectively be modeled as any other loss process.

Now, let us provide a brief description of the physics of this process. Firstly, the detection time-window is chosen such that the probability of detecting a photon from the optical excitation pulse used to entangle the electron spin with the photonic qubit is negligible [156]. For that reason the detection time-window is opened after a fixed offset $t_{\mathrm{w}}^{\mathrm{offset}}$ with respect to the beginning of the decay of the optical excited state of the electron spin. We note that for the considered enhancement of the ZPL-emission using the optical cavity we predict the characteristic time of the NV emission τ to be approximately a half of the corresponding value of τ if no cavity is used [156, 198, 183]. Therefore here we consider the scenario where the duration of the optical excitation pulse is made twice shorter with respect to the one used in [156]. This will allow us to filter out the unwanted photons from the excitation pulse by setting $t_{\mathrm{w}}^{\mathrm{offset}}$ to half of the offset used in [156].

Secondly, we note that the detection time-window cannot last too long, specifically, it needs to be chosen such that there is a good trade-off between detecting coherent and non-coherent (i.e. dark counts) photons. In this subsection we will discuss the effects of photons arriving outside of this time-window and the effects of registering dark counts within this time-window.

A.1.0.1 Losses from the detector time-window

The NV center emits a photon through an exponential decay process with characteristic time τ. Therefore the probability of detecting a photon during a time-window starting at $t_{\mathrm{w}}^{\mathrm{offset}}$ and lasting for t_{w} is

$$p_{\mathrm{in}}(t_{\mathrm{w}}) = \frac{1}{\tau}\int_{t_{\mathrm{w}}^{\mathrm{offset}}}^{t_{\mathrm{w}}^{\mathrm{offset}}+t_{\mathrm{w}}} \mathrm{d}t \exp\left(-\frac{t}{\tau}\right) = \exp\left(-\frac{t_{\mathrm{w}}^{\mathrm{offset}}}{\tau}\right) - \exp\left(-\frac{t_{\mathrm{w}}^{\mathrm{offset}}+t_{\mathrm{w}}}{\tau}\right) . \tag{A.2}$$

Clearly the process of a photon arriving outside of the time-window is qualitatively different from the loss process where the photons get lost to the environment. In the remainder of this section we will now look at the difference between these two phenomena in more detail.

The emission process of the NV center is a coherent process over time. Consider a generic scenario in which we divide the emission time into two intervals, denoted by "in" and "out", respectively. Coherent emission then means that the state of the photon emitted by the electron spin in state $|\uparrow\rangle$ will be

$$|\psi\rangle = \sqrt{p_{\mathrm{in}}}\,|1\rangle_{\mathrm{in}}\,|0\rangle_{\mathrm{out}} + \sqrt{1-p_{\mathrm{in}}}\,|0\rangle_{\mathrm{in}}\,|1\rangle_{\mathrm{out}} \ . \tag{A.3}$$

Now let us come back to our specific model, in which the "in" mode corresponds to the interval $\left[t_{\mathrm{w}}^{\mathrm{offset}},\ t_{\mathrm{w}}^{\mathrm{offset}}+t_{\mathrm{w}}\right]$ and the "out" mode to all the times $t \geq 0$ lying outside of this interval ($t = 0$ is the earliest possible emission time). Here, the emission into the "in" mode occurs with probability $p_{\mathrm{in}}(t_{\mathrm{w}})$. Hence the spin-photon state resulting from the emission by the $\alpha\,|\downarrow\rangle + \beta\,|\uparrow\rangle$ spin state is

$$|\psi\rangle = \alpha\,|\downarrow\rangle\,|0\rangle_{\mathrm{in}}\,|0\rangle_{\mathrm{out}} + \beta\,|\uparrow\rangle\left(\sqrt{p_{\mathrm{in}}(t_{\mathrm{w}})}\,|1\rangle_{\mathrm{in}}\,|0\rangle_{\mathrm{out}} + \sqrt{1-p_{\mathrm{in}}(t_{\mathrm{w}})}\,|0\rangle_{\mathrm{in}}\,|1\rangle_{\mathrm{out}}\right) . \tag{A.4}$$

If the presence-absence encoding is used, such a photonic qubit is then transmitted to the detector. Since only the spin and the "in" mode of the photon will be measured, we can now trace out the "out" mode

$$\rho = \left(|\alpha|^2 + |\beta|^2 p_{\text{in}}(t_{\text{w}})\right) |\phi\rangle\langle\phi| + |\beta|^2 (1 - p_{\text{in}}(t_{\text{w}})) \, |\uparrow\rangle\langle\uparrow| \otimes |0\rangle\langle 0|_{\text{in}} \ , \tag{A.5}$$

where

$$|\phi\rangle = \frac{1}{\sqrt{|\alpha|^2 + |\beta|^2 p_{\text{in}}(t_{\text{w}})}} \left(\alpha \, |\downarrow\rangle \, |0\rangle_{\text{in}} + \beta \sqrt{p_{\text{in}}(t_{\text{w}})} \, |\uparrow\rangle \, |1\rangle_{\text{in}}\right) \ . \tag{A.6}$$

Note that this state can be obtained by passing the photonic qubit of the state

$$|\psi\rangle = \alpha \, |\downarrow\rangle \, |0\rangle + \beta \, |\uparrow\rangle \, |1\rangle \ , \tag{A.7}$$

through the amplitude-damping channel with the damping parameter given by $1 - p_{\text{in}}(t_{\text{w}})$. Hence we can conclude that for the photon number encoding, the possibility of the photon arriving outside of the time-window of the detector can be modeled in the same way as any other photon loss process, namely an amplitude-damping channel applied to that photonic qubit.

In the case of time-bin encoding we effectively have four photonic qubits, since now we have an "in" and "out" mode for both the early (denoted by "e") and the late (denoted by "l") time-window. We assume here that the slots do not overlap. That is, a photon emitted in the "out" mode of the early time-window is always distinct from any photon in the late time-window. This can be achieved by making the time gap between the "in" modes of the early and late window long enough. In this case the emission process results in a state

$$|\psi\rangle = \alpha \, |\downarrow\rangle \left(\sqrt{p_{\text{in}}(t_{\text{w}})} \, |1\rangle_{e,\text{in}} \, |0\rangle_{e,\text{out}} \, |0\rangle_{l,\text{in}} \, |0\rangle_{l,\text{out}} + \sqrt{1 - p_{\text{in}}(t_{\text{w}})} \, |0\rangle_{e,\text{in}} \, |1\rangle_{e,\text{out}} \, |0\rangle_{l,\text{in}} \, |0\rangle_{l,\text{out}}\right) \tag{A.8}$$

$$+ \beta \, |\uparrow\rangle \left(\sqrt{p_{\text{in}}(t_{\text{w}})} \, |0\rangle_{e,\text{in}} \, |0\rangle_{e,\text{out}} \, |1\rangle_{l,\text{in}} \, |0\rangle_{l,\text{out}} + \sqrt{1 - p_{\text{in}}(t_{\text{w}})} \, |0\rangle_{e,\text{in}} \, |0\rangle_{e,\text{out}} \, |0\rangle_{l,\text{in}} \, |1\rangle_{l,\text{out}}\right) \ . \tag{A.9}$$

Again, tracing out the "out" modes results in a state

$$\rho = p_{\text{in}}(t_{\text{w}}) \, |\phi\rangle\langle\phi| + (1 - p_{\text{in}}(t_{\text{w}})) \left(|\alpha|^2 \, |\downarrow\rangle\langle\downarrow| + |\beta|^2 \, |\uparrow\rangle\langle\uparrow|\right) \otimes |00\rangle\langle 00|_{e,l} \ , \tag{A.10}$$

where

$$|\phi\rangle = \alpha \, |\downarrow\rangle \, |1\rangle_e \, |0\rangle_l + \beta \, |\uparrow\rangle \, |0\rangle_e \, |1\rangle_l = \alpha \, |\downarrow\rangle \, |e\rangle + \beta \, |\uparrow\rangle \, |l\rangle \ . \tag{A.11}$$

Here $|00\rangle_{e,l}$ corresponds to the loss flag from which we see that for the time-bin encoding the possible arrival of a photon outside of the time-window results in an erasure channel with the erasure probability given by $(1 - p_{\text{in}}(t_{\text{w}}))$. Hence this process can be also modeled as any other loss process for this encoding.

We have just shown that for both photon presence/absence and time-bin encodings the process of the photon arriving outside of the time-window can be modeled by the source which prepares photons in a coherent superposition of the "in" and "out" modes and the detector tracing out (losing) the "out" modes. We have also shown that those two elements combined together result effectively in a loss process corresponding to the same channel as any other loss process for that encoding (amplitude-damping for photon presence/absence and erasure channel for time-bin encoding).

However, between the source and the detector there are other lossy or noisy components resulting in other quantum channels that need to be applied before the tracing out of the "out" mode at the detector. Now we show that for all loss and noise processes that occur in our model, the tracing out of the "out" mode can be mathematically commuted through all those additional noise/lossy processes. This means that the tracing out can be applied directly after the source, such that the above described reductions to amplitude-damping or erasure channel can be applied.

Consider the quantum channels acting on the photonic qubits of the form

$$\mathcal{N} = \sum_i p_i \mathcal{N}^i_{\text{in}} \otimes \mathcal{N}^i_{\text{out}} \ . \tag{A.12}$$

Effectively these are the channels that do not couple the "in" and "out" modes. Since in reality "in" and "out" modes correspond to different time modes, their coupling would require some kind of memory inside the channel. Hence we can think of the above defined channels as channels without memory. Now it is clear that for a quantum state ρ that among its registers includes both the "in" and the "out" mode, we have that

$$\text{tr}_{\text{out}}[\mathcal{N}(\rho)] = \text{tr}_{\text{out}}\left[\sum_i p_i \mathcal{N}^i_{\text{in}} \otimes \mathcal{N}^i_{\text{out}}(\rho)\right] = \sum_i p_i \mathcal{N}^i_{\text{in}}(\rho_{\text{in}}) \ . \tag{A.13}$$

Now, firstly tracing out the "out" modes and then applying the channel $\mathcal{N}$ (only the "in" part can be applied now) also results in $\sum_i p_i \mathcal{N}^i_{\text{in}}(\rho_{\text{in}})$ at the output. Hence the tracing out of the "out" modes commutes with all the channels that are of the form (A.12), which correspond to channels without memory. Clearly the noise/loss processes that occur before the detection, such as photon loss or dephasing due to uncertainty in the optical phase of the photon, belong to this class of channels. In particular this means that for photon presence/absence the amplitude-damping due to photon loss in the channel and due to photon arrival outside of the time-window can be both combined into one channel with the single damping parameter given by $1 - \eta p_{\text{in}}(t_{\text{w}})$ (η denotes the transmissivity due to the loss process e.g. the transmissivity of the fiber). The same applies to time-bin encoding where we now have a single erasure channel with erasure probability $1 - \eta p_{\text{in}}(t_{\text{w}})$.

To conclude, the arrival of the photon outside of the time-window can be modeled in the same way as any other loss process for both photon encodings used and therefore we can now redefine the detector efficiency $p'_{\text{det}} = p_{\text{det}} \cdot p_{\text{in}}(t_{\text{w}})$ and the total apparatus efficiency $p'_{\text{app}} = p_{\text{ce}} p_{\text{zpl}} p'_{\text{det}}$. We can then define $\eta_{\text{total}} = p'_{\text{app}} \eta_f$ as the total transmissivity - with probability η_{total} a photon will be successfully transmitted from the sender to the receiver.

A.1.0.2 Dark counts within the detector time-window

Photon detectors are imperfect, and due to thermal excitations, they will register clicks that do not correspond to any incoming photons. These undesired clicks are called dark counts and can effectively be seen as a source of noise. The magnitude of this noise depends on the ratio between the probability of detecting the signal photon and measuring a dark count. Clearly, dark counts become a dominant source of noise when the probability of detecting the signal photon becomes comparable to the probability of a dark count click. The probability p_d of getting at least one dark count within the time-window t_{w} of awaiting the signal photon is given by $p_d = 1 - \exp(-t_{\text{w}} \cdot \text{DCpS})$, where DCpS is the number of dark count per second of the detector [23].

In the SiSQuRe scheme Alice and Bob perform measurements on time-bin encoded photons. The same applies to Bob in the SPADS scheme. Since at least two detectors are required to perform this measurement, the presence of dark counts means that the outcome may lie outside of the qubit space. Moreover, this measurement needs to be trusted. In consequence, a squashing map needs to be used to process the multi-click events in a secure way. Here as an approximation we consider the squashing map for the polarization encoding [227] in the same way as described in [23]. Hence this measurement can also be modeled as a perfect measurement preceded by a depolarizing channel with parameter α which depends on whether the BB84 or six-state protocol is used. The parameter α is given by [23]:

$$\alpha_{A/B,\ \mathrm{BB84}} = \frac{p'_{\mathrm{app}}\eta_B(1-p_d)}{1-(1-p'_{\mathrm{app}}\eta_{A/B})(1-p_d)^2} \ , \tag{A.14}$$

$$\alpha_{A/B,\ \text{six-state}} = \frac{p'_{\mathrm{app}}\eta_{A/B}(1-p_d)^5}{1-(1-p'_{\mathrm{app}}\eta_{A/B})(1-p_d)^6} \ . \tag{A.15}$$

Here $\eta_{A/B}$ denotes the transmissivity of the fiber between the memory repeater node and Alice's/Bob's detector setup. Finally we note that dark counts increase the probability of registering a successfull measurement event. For the optical measurement schemes utilising the squashing map the probability of registering a click in at least one detector is given by [23]:

$$p_{A/B,\ BB84} = 1-(1-p'_{\mathrm{app}}\eta_{A/B})(1-p_d)^2 \ , \tag{A.16}$$

$$p_{A/B,\ \text{six-state}} = 1-(1-p'_{\mathrm{app}}\eta_{A/B})(1-p_d)^6 \ . \tag{A.17}$$

The effect of dark counts in the single-photon scheme, which carries over to the SPOTL scheme, is analyzed in Appendix A.5.

Noise due to optical phase uncertainty

Another important noise process affecting photonic qubits is related to the fact that for the photon presence/absence encoding the spin-photon entangled state will also depend on the optical phase of the apparatus used. Specifically, it will depend on the phase of the lasers used to generate the spin photon entanglement as well as the optical phase acquired by the photons during the transmission of the photonic qubit. Knowledge about this phase is crucial for being able to generate entanglement through the single-photon scheme. In any realistic setup however, there would be a certain degree of the lack of knowledge about this phase acquired by the photons. Since in the end what matters is the knowledge about the relative phase between the two photons, we can model this source of noise as the lack of knowledge of the phase on only one of the incoming photonic qubits. This noise process can be effectively modeled as dephasing. In this section we will show that the phase uncertainty induces dephasing with a parameter λ equal to

$$\lambda = \frac{I_1\left(\frac{1}{(\Delta\phi)^2}\right)}{2I_0\left(\frac{1}{(\Delta\phi)^2}\right)} + \frac{1}{2} \ , \tag{A.18}$$

where $\Delta\phi$ is the uncertainty in the phase and $I_{0/1}$ is the Bessel function of order 0/1. Let us assume that for Alice, the local phase of the photonic qubit has a Gaussian-like distribution on a circle, with standard deviation $\Delta\phi$ as observed in [142]. This motivates us to model the distribution as a von Mises

distribution [228]. The von Mises distribution reads

$$f(\phi) = \frac{e^{\kappa \cos(\phi-\mu)}}{2\pi I_0(\kappa)} \ . \tag{A.19}$$

Here μ is the measure of location, i.e. it corresponds to the center of the distribution, κ is a measure of concentration and can be effectively seen as the inverse of the variance and I_0 is the modified Bessel function of the first kind of order 0. One can then show [228] that

$$\int_{-\pi}^{\pi} \mathrm{d}\phi f(\phi) e^{\pm i\phi} = \frac{I_1(\kappa)}{I_0(\kappa)} e^{\pm i\mu} \ . \tag{A.20}$$

Since we are only interested in the noise arising from the lack of knowledge about the phase rather than the actual value of this phase, without loss of generality we can assume $\mu = 0$. Moreover, the experimental parameter that we use here is effectively the standard deviation of the distribution $\Delta\phi$ and therefore we can write $\kappa = \frac{1}{(\Delta\phi)^2}$.

Hence, let us write the spin-photon entangled state that depends on the optical phase ϕ.

$$\left|\psi^{\pm}(\phi)\right\rangle = \sin(\theta) \left|\downarrow 0\right\rangle \pm e^{i\phi} \cos(\theta) \left|\uparrow 1\right\rangle \ . \tag{A.21}$$

Now, the lack of knowledge about this phase leads to a mixed state:

$$\begin{aligned} \int_{-\pi}^{\pi} f(\phi) \left|\psi^{\pm}(\phi)\right\rangle\!\!\left\langle\psi^{\pm}(\phi)\right| \mathrm{d}\phi = \sin^2(\theta) \left|\downarrow 0\right\rangle\!\!\left\langle\downarrow 0\right| + \cos^2(\theta) \left|\uparrow 1\right\rangle\!\!\left\langle\uparrow 1\right| \\ \pm \sin(\theta)\cos(\theta) \int_{-\pi}^{\pi} f(\phi)(e^{i\phi} \left|\uparrow 1\right\rangle \left\langle\downarrow 0\right| + e^{-i\phi} \left|\downarrow 0\right\rangle \left\langle\uparrow 1\right|)\mathrm{d}\phi \ . \end{aligned} \tag{A.22}$$

Let us now try to map this state onto a dephased state

$$\begin{aligned} \lambda \left|\psi^{\pm}(0)\right\rangle\!\!\left\langle\psi^{\pm}(0)\right| + (1-\lambda) \left|\psi^{\mp}(0)\right\rangle\!\!\left\langle\psi^{\mp}(0)\right| = \sin^2(\theta) \left|\downarrow 0\right\rangle\!\!\left\langle\downarrow 0\right| + \cos^2(\theta) \left|\uparrow 1\right\rangle\!\!\left\langle\uparrow 1\right| \\ \pm \sin(\theta)\cos(\theta)(2\lambda-1)(\left|\uparrow 1\right\rangle \left\langle\downarrow 0\right| + \left|\downarrow 0\right\rangle \left\langle\uparrow 1\right|) \ . \end{aligned} \tag{A.23}$$

Hence, we observe that

$$2\lambda - 1 = \frac{I_1\left(\frac{1}{(\Delta\phi)^2}\right)}{I_0\left(\frac{1}{(\Delta\phi)^2}\right)} \ . \tag{A.24}$$

$$\rightarrow \lambda = \frac{I_1\left(\frac{1}{(\Delta\phi)^2}\right)}{2I_0\left(\frac{1}{(\Delta\phi)^2}\right)} + \frac{1}{2} \ . \tag{A.25}$$

A.2 Noisy processes in NV-based quantum memories

In our setups we use ^{13}C nuclear spins in diamond as long-lived memory qubits next to a Nitrogen Vacancy (NV) electron spin taking the role of a communication qubit. In this Appendix, we will detail our model of the noisy processes in the NV.

The electron spin can be manipulated via microwave pulses and an optical pulse is used to create and send a photon entangled with it. This operation is noisy and can be modeled as having a dephasing noise of parameter F_{prep}. This means that, if the desired generated target state between the photon and the

electron spin was $|\psi^+\rangle$, we actually have a mixture $F_{\text{prep}}\,|\psi^+\rangle\langle\psi^+| + (1-F_{\text{prep}})(\mathbb{I}\otimes Z)\,|\psi^+\rangle\langle\psi^+|\,(\mathbb{I}\otimes Z)$. Information can be stored via a swapping of the electron spin state to the long living nuclear ^{13}C spin. Through this swap operation we also free the communication qubit to be used for consecutive remote entanglement generation attempts. Due to interaction with its environment, a quantum state stored in a ^{13}C spin quantum memory undergoes an evolution that we model with a dephasing and a depolarizing channel with noise parameters $\lambda_1 = (1+e^{-an})/2$ and $\lambda_2 = e^{-bn}$, respectively. The form of the parameters a and b in general depends on the scheme. For the SiSQuaRe, SPADS the SPOTL schemes there are two distinct effects that cause this decoherence: one induced by the time it takes to generate entanglement between the middle node and Bob, and one induced by the always-on hyperfine coupling between the electron spin and the carbon spin inside the middle NV node. This coupling becomes an additional source of decoherence for the carbon spin during probabilistic attempts to generate remote entanglement using the electron spin [147, 167]. We model the decoherence effect on the qubit stored in the carbon spin of the middle node by a dephasing channel with parameter λ_1,

$$\mathcal{D}^{\lambda_1}_{\text{dephase}}(\rho) = \lambda_1\rho + (1-\lambda_1)Z\rho Z\ , \tag{A.26}$$

and depolarizing channel with parameter λ_2,

$$\mathcal{D}^{\lambda_2}_{\text{depol}}(\rho) = \lambda_2\rho + (1-\lambda_2)\frac{\mathbb{I}}{d}\ , \tag{A.27}$$

where λ_1 and λ_2 quantify the noise. The parameters depend as follows on the number of attempts n,

$$\lambda_1 = F_{T_2} = \frac{1+e^{-an}}{2}\ , \tag{A.28}$$

$$\lambda_2 = F_{T_1} = e^{-bn}\ , \tag{A.29}$$

where a and b are given by

$$a = a_0 + a_1\left(L_s\cdot\frac{n_{ri}}{c} + t_{\text{prep}}\right)\ , b = b_0 + b_1\left(L_s\cdot\frac{n_{ri}}{c} + t_{\text{prep}}\right)\ . \tag{A.30}$$

Here n_{ri} is the refractive index of the fiber, c is the speed of light in vacuum, t_{prep} is the time it takes to prepare for the emission of an entangled photon and L_s is the distance the signal needs to travel before the repeater receives the information about failure or success of the attempt. Let L_B denote the distance between the memory repeater node and Bob. Then for the SiSQuaRe and SPADS schemes $L_s = 2L_B$ as in each attempt first the quantum signal needs to travel to Bob who then sends back to the middle node the classical information about success or failure. For the SPOTL scheme $L_s = L_B$ as in this case both the quantum and the classical signals need to travel only half of the distance between the middle node and Bob since the signals are exchanged with the heralding station which is located half-way between the middle memory node and Bob. The parameters a_0 and b_0 quantify the noise due to a single attempt at generating an entangled spin-photon, induced by stochastic electron spin reset operations, quasi static noise and microwave control infidelities. The parameters a_1 and b_1 quantify the noise during storage per second.

Gates and measurements in the quantum memory are also imperfect. We model those imperfections via two depolarizing channels. The first one acts on a single qubit with depolarizing parameter $\lambda_2 = F_m$ corresponding to the measurement of the electron spin. The second one acts on two qubits with depolarizing parameter $\lambda_2 = F_g$ corresponding to applying a two-qubit gate to both the electron spin

and the ^{13}C spin. This means that every time a measurement is done on a e^- qubit of a quantum state ρ, it is actually done on $\mathcal{D}^{F_m}_{\text{depol}}(\rho)$. Also a swapping operation between the e^- spin and the nuclear spin (done experimentally via two two-qubit gates, see main text) leads to an error modeled by a depolarizing channel of parameter $F_{\text{swap}} = F_g^2$. Following the same logic, a Bell state measurement will cause the state to undergo an evolution given by a depolarizing channel. Specifically, following the decomposition of the Bell measurement into elementary gates for the NV-implementation as described in Section 4.3, this evolution will consist of a depolarizing channel with parameter F_g^2 acting on both of the measured qubits and the depolarizing channel with parameter F_m^2 acting only on the electron spin qubit.

A.3 Expectation of the number of channel uses with a cut-off

In this Appendix we derive an analytical formula for the expectation value of the number of channel uses between Alice and Bob needed to generate one bit of raw key for the SiSQuaRe, SPADS and SPOTL schemes,

$$\mathbb{E}[N] = \frac{1}{p_A \cdot (1-(1-p_B)^{n^*})} + \frac{1}{p_B} \ . \tag{A.31}$$

For these three schemes, we implement a cut-off which is used to prevent decoherence. Each time the number of channel uses between the repeater node and Bob reaches the cut-off n^*, the entire protocol restarts from the beginning. Here we take a conservative view and define the number of channel uses N between Alice and Bob as the sum $N_A + N_B$, where N_A (N_B) corresponds to the number of channel uses between Alice (Bob) and the middle node. From the linearity of the expectation value we have that

$$\mathbb{E}[N_A + N_B] = \mathbb{E}[N_A] + \mathbb{E}[N_B] \ . \tag{A.32}$$

We denote by p_A and p_B the probability of a successful attempt on Alice's and Bob's side respectively. Bob's number of channel uses follows a geometric distribution with parameter $p = p_B$, so that $\mathbb{E}[N_B] = \frac{1}{p_B}$. Without the cut-off, Alice's number of channel uses would follow a geometric distribution with parameter $p = p_A$. However, the cut-off parameter adds additional channel uses on Alice side. Since the probability that Bob succeeds within n^* trials is $p_{\text{succ}} = 1-(1-p_B)^{n^*}$, we in fact have that Alice's number of channel uses follows a geometric distribution with parameter $p'_A = p_A \cdot p_{\text{succ}}$. Hence it is straightforward to see that

$$\mathbb{E}[N_A + N_B] = \frac{1}{p'_A} + \frac{1}{p_B} \tag{A.33}$$

$$= \frac{1}{p_A \cdot (1-(1-p_B)^{n^*})} + \frac{1}{p_B} \ . \tag{A.34}$$

A.4 SiSQuaRe scheme analysis

The analysis of the SiSQuare scheme has been performed in [23]. In this work we use the estimates of the yield and QBER as derived in [23] with the following modifications:

- For the calculation of the yield we now adopt a conservative perspective and calculate the number of channel uses as $\mathbb{E}[N_A + N_B]$, as derived in Appendix A.3, rather than $\mathbb{E}[\max(N_A, N_B)]$. Note that $\mathbb{E}[\max(N_A, N_B)] \leq \mathbb{E}[N_A + N_B] \leq 2\mathbb{E}[\max(N_A, N_B)]$.
- The total depolarising parameter for gates and measurements F_{gm} defined in [23] is now decomposed into individual operations as described in Appendix A.2. That is, in this work depolarisation due to imperfect operations on the memories is expressed in terms of depolarising parameter due to imperfect measurement, F_m, and imperfect two-qubit gate, F_g. Since in the analysis of the SiSQuaRe scheme we only deal with Bell diagonal states, the overall noise due to imperfect swap gate and the Bell measurement leads to $F_{\text{gm}} = F_g^4 F_m^2$.
- In [23] we have assumed the duration of the detection time-window to be fixed to 30 ns and assumed that all the emitted photons will fall into that time-window. Here, similarly as for other schemes, we perform a more refined analysis in which we include the trade-off between the duration of the time-window and the dark count probability as described in Appendix A.1.

A.5 Single-photon scheme analysis

In this Appendix we provide a detailed analysis of the single-photon scheme between two remote NV-center nodes. This section is structured as follows. First, we describe the creation of the spin-photon entangled state followed by the action of the lossy channel on the photonic part of this state, including the noise due to the uncertainty in the phase of the state induced by the fiber. Second, we apply the optical Bell measurement. Then we evaluate the effect of dark counts which introduce additional errors to the generated state. Finally we calculate the yield of this scheme and extract the QBER from the resulting state.

Spin-photon entanglement and action of a lossy fiber on the photonic qubit

Firstly, both Alice and Bob generate spin-photon entangled states, parameterized by θ. As we will later see, this parameter allows for trading off the quality of the final entangled state of the two spins with the yield of the generation process. The ideal spin-photon state would then be described as

$$\left|\psi^+\right\rangle = \sin(\theta)\left|\downarrow\right\rangle\left|0\right\rangle + \cos(\theta)\left|\uparrow\right\rangle\left|1\right\rangle \ . \tag{A.35}$$

The preparation of the spin-photon entangled state is not ideal. That is, the spin-photon entangled state is not actually as described above, but rather of the form (see Appendix A.2)

$$\begin{aligned}\rho &= F_{\text{prep}}\left|\psi^+\right\rangle\!\left\langle\psi^+\right| + (1-F_{\text{prep}})(\mathbb{I}\otimes Z)\left|\psi^+\right\rangle\!\left\langle\psi^+\right|(\mathbb{I}\otimes Z) \\ &= F_{\text{prep}}\left|\psi^+\right\rangle\!\left\langle\psi^+\right| + (1-F_{\text{prep}})\left|\psi^-\right\rangle\!\left\langle\psi^-\right| \ .\end{aligned} \tag{A.36}$$

Here

$$\left|\psi^-\right\rangle = \sin(\theta)\left|\downarrow\right\rangle\left|0\right\rangle - \cos(\theta)\left|\uparrow\right\rangle\left|1\right\rangle \ . \tag{A.37}$$

For the next step we need to consider two additional noise processes that affect the photonic qubits before the optical Bell measurement is performed. The first one is the loss of the photonic qubit. This can happen at the emission, while filtering the photons that are not of the required ZPL frequency, in the lossy fiber, in the imperfect detectors, or due to the arrival outside of the time window in which detectors expect a click. All these losses can be combined into a single loss parameter

$$\eta = \eta_{\text{total}} = p_{\text{ce}} p_{\text{zpl}} \sqrt{\eta_f} p'_{\text{det}} \ , \tag{A.38}$$

with $\eta_f = \exp\left(-\frac{L}{L_0}\right)$, where L is the distance between the two remote NV-center nodes in the scheme (see Fig. 4.6 and Appendix A). Hence, a photon is successfully transmitted through the fiber and detected in the middle heralding station with probability η. Now we note that the action of the pure-loss channel on the qubit encoded in the presence or absence of a photon corresponds to the action of the amplitude-damping channel with the damping parameter $1-\eta$ [226].

The second process that effectively happens at the same time as loss, is the dephasing noise arising from the optical instability of the apparatus as described in Appendix A.1. We note that the amplitude-damping and dephasing channel commute, hence it does not matter in which order we apply the two noise processes corresponding to the loss of the photonic qubit and unknown drifts of the phase of the photonic qubit in our model. Here we firstly apply the dephasing due to the lack of knowledge of the phase on Alice's photon and then amplitude-damping on both photons due to all the loss processes.

Following the model in Appendix A.1, the lack of knowledge about the optical phase will effectively transform Alice's state to

$$\rho_A = (F_{\text{prep}}\lambda + (1-F_{\text{prep}})(1-\lambda)) \left|\psi^+\right\rangle\!\left\langle\psi^+\right| + ((1-F_{\text{prep}})\lambda + F_{\text{prep}}(1-\lambda)) \left|\psi^-\right\rangle\!\left\langle\psi^-\right| \ . \tag{A.39}$$

where

$$\lambda = \frac{I_1\left(\frac{1}{(\Delta\phi)^2}\right)}{2I_0\left(\frac{1}{(\Delta\phi)^2}\right)} + \frac{1}{2}. \tag{A.40}$$

Now we can apply all the transmission losses modeled as the amplitude-damping channel. The action of this channel on the photonic part of the state ρ results in the state that we can describe as follows. Firstly, let us introduce two new states

$$\left|\psi_\eta^\pm\right\rangle = \frac{1}{\sqrt{\sin^2(\theta) + \eta\cos^2(\theta)}} (\sin(\theta)\left|\downarrow\right\rangle\left|0\right\rangle \pm \sqrt{\eta}\cos(\theta)\left|\uparrow\right\rangle\left|1\right\rangle) \ . \tag{A.41}$$

Then, after the losses and before the Bell measurement, the state of Alice can be written as

$$\begin{aligned}\rho'_A = {} & \left(\sin^2(\theta) + \eta\cos^2(\theta)\right)\left((F_{\text{prep}}\lambda + (1-F_{\text{prep}})(1-\lambda))\left|\psi_\eta^+\right\rangle\!\left\langle\psi_\eta^+\right| + ((1-F_{\text{prep}})\lambda + F_{\text{prep}}(1-\lambda))\left|\psi_\eta^-\right\rangle\!\left\langle\psi_\eta^-\right|\right) \\ & + (1-\eta)\cos^2(\theta)\left|\uparrow\right\rangle\!\left\langle\uparrow\right|\left|0\right\rangle\!\left\langle 0\right| \ ,\end{aligned} \tag{A.42}$$

and for Bob

$$\rho'_B = \left(\sin^2(\theta) + \eta\cos^2(\theta)\right)\left(F_{\text{prep}}\left|\psi_\eta^+\right\rangle\!\left\langle\psi_\eta^+\right| + (1-F_{\text{prep}})\left|\psi_\eta^-\right\rangle\!\left\langle\psi_\eta^-\right|\right) + (1-\eta)\cos^2(\theta)\left|\uparrow\right\rangle\!\left\langle\uparrow\right|\left|0\right\rangle\!\left\langle 0\right| \ . \tag{A.43}$$

States after the Bell measurement

Now we need to perform a Bell measurement on the photonic qubits within the states ρ'_A and ρ'_B. Here we consider the scenario with non photon-number resolving detectors. Assuming for the moment the scenario without dark counts, we have at most two photons in the system. Hence we can consider three possible outcomes of our optical measurement: left detector clicked, right detector clicked, none of the detectors clicked. The measurement operators can be easily derived by noting that in our scenario without dark counts, each of the detectors can be triggered either by one or two photons and no cross-clicks between detectors are possible due to the photon-bunching effect. Then we can apply the reverse of the beam splitter mode transformations to the projectors on the events with one or two photons in each of the detectors to obtain these projectors in terms of the input modes. Finally we truncate the resulting projectors to the qubit space since in our scenario it is not possible for more than one photon to be present in each of the input modes of the beam splitter. In this way we obtain the following measurement operators

$$\begin{aligned} A_0 &= \left|\Psi^+\right\rangle\!\left\langle\Psi^+\right| + \frac{1}{\sqrt{2}}\left|11\right\rangle\!\left\langle 11\right| \ , \\ A_1 &= \left|\Psi^-\right\rangle\!\left\langle\Psi^-\right| + \frac{1}{\sqrt{2}}\left|11\right\rangle\!\left\langle 11\right| \ , \\ A_2 &= \left|00\right\rangle\!\left\langle 00\right| \ . \end{aligned} \tag{A.44}$$

These outcomes occur with the following probabilities,

$$p_0 = p_1 = \eta\cos^2(\theta)\left(1 - \frac{\eta}{2}\cos^2(\theta)\right) \ , \tag{A.45}$$

$$p_2 = (1 - \eta\cos^2(\theta))^2 \ . \tag{A.46}$$

The post-measurement state of the two spins for the outcome A_0 is

$$\rho_0 = \frac{2\sin^2(\theta)}{2 - \eta\cos^2(\theta)}\left(a\left|\Psi^+\right\rangle\!\left\langle\Psi^+\right| + b\left|\Psi^-\right\rangle\!\left\langle\Psi^-\right|\right) + \frac{\cos^2(\theta)(2-\eta)}{2 - \eta\cos^2(\theta)}\left|\uparrow\uparrow\right\rangle\!\left\langle\uparrow\uparrow\right| \ . \tag{A.47}$$

Here

$$\left|\Psi^\pm\right\rangle = \frac{1}{\sqrt{2}}\left(\left|\downarrow\uparrow\right\rangle \pm \left|\uparrow\downarrow\right\rangle\right) \ , \tag{A.48}$$

$$a = \lambda(F_{\text{prep}}^2 + (1 - F_{\text{prep}})^2) + 2F_{\text{prep}}(1 - F_{\text{prep}})(1 - \lambda) \ , \tag{A.49}$$

$$b = (1 - \lambda)(F_{\text{prep}}^2 + (1 - F_{\text{prep}})^2) + 2F_{\text{prep}}(1 - F_{\text{prep}})\lambda \ . \tag{A.50}$$

For the outcome A_1 the post-measurement state of the spins is the same up to a local Z gate which Bob can apply following the trigger of the A_1 outcome. The post-measurement state of the spins for the outcome A_2, that is when none of the detector clicked, is

$$\rho_2 = \frac{1}{(1 - \eta\cos^2(\theta))^2}\left(\sin^4(\theta)\left|\downarrow\downarrow\right\rangle\!\left\langle\downarrow\downarrow\right| + (1-\eta)\cos^2(\theta)\sin^2(\theta)\left(\left|\downarrow\uparrow\right\rangle\!\left\langle\downarrow\uparrow\right| + \left|\uparrow\downarrow\right\rangle\!\left\langle\uparrow\downarrow\right|\right) + (1-\eta)^2\cos^4(\theta)\left|\uparrow\uparrow\right\rangle\!\left\langle\uparrow\uparrow\right|\right) \ . \tag{A.51}$$

This is a separable state and so events corresponding to outcome A_2 (that is, no click in any of the detectors) will be discarded as failure. However, dark counts on our detectors can make us draw wrong conclusions about which of the three outcomes we actually obtained.

The effect of dark counts can be seen as follows

- We measured A_2 (no actual detection) but one of the detectors had a dark count. This event will happen with probability $2p_2p_d(1-p_d)$ and will make us accept the state ρ_2. Note that this is a classical state so application of the Z correction by Bob does not affect this state at all.
- We measured A_1 or A_2 but we also got a dark count in the other detector. This event will happen with probability $(p_0+p_1)\cdot p_d$. This will effectively lead us to rejection of the desired state ρ_0. Hence effectively ρ_0 will only be accepted if we measured A_1 or A_2 but the other detector did not have a dark count, which will happen with probability $(p_0+p_1)\cdot(1-p_d)$.

The yield and QBER

Taking dark counts into account, we see that the yield of the single-photon scheme, which is just the probability of registering a click in only one of the detectors, will be

$$\begin{aligned} Y &= (p_0+p_1)(1-p_d)+2p_2p_d(1-p_d) \\ &= 2(1-p_d)\left[\eta\cos^2(\theta)\left(1-\frac{\eta}{2}\cos^2(\theta)\right)+(1-\eta\cos^2(\theta))^2p_d\right] . \end{aligned} \tag{A.52}$$

The effective accepted state after a click in one of the detectors will then be

$$\rho_{\text{out}} = \frac{1}{Y}\left((p_0+p_1)(1-p_d)\rho_0+2p_2p_d(1-p_d)\rho_2\right) . \tag{A.53}$$

Note that both Alice and Bob perform a measurement on their electron spins immediately after each of the spin-photon entanglement generation events. This measurement causes an error modeled as a depolarizing channel of parameter F_m on each qubit, which means that after a successful run of the single-photon protocol, the effective state shared by Alice and Bob including the noise of their measurements will be given by

$$\rho_{AB} = F_m^2\rho_{\text{out}}+(1-F_m)F_m\left[\frac{\mathbb{I}_{2,A}}{2}\otimes \text{tr}_A[\rho_{\text{out}}]+\text{tr}_B[\rho_{\text{out}}]\otimes\frac{\mathbb{I}_{2,B}}{2}\right]+(1-F_m)^2\,\frac{\mathbb{I}_{4,AB}}{4} . \tag{A.54}$$

One can then extract the QBER for this state in all the three bases using the appropriate correlated/anti-correlated projectors such that:

$$e_z = \text{Tr}((|00\rangle\langle 00|+|11\rangle\langle 11|)\rho_{AB}) , \tag{A.55}$$

$$e_{xy} = \text{Tr}((|+-\rangle\langle +-|+|-+\rangle\langle -+|)\rho_{AB}) = \text{Tr}((|0_y1_y\rangle\langle 0_y1_y|+|1_y0_y\rangle\langle 1_y0_y|)\rho_{AB}) . \tag{A.56}$$

Here $|+\rangle$ and $|-\rangle$ denote the two eigenstates of X and $|0_y\rangle$ and $|1_y\rangle$ denote the two eigenstates of Y. We note that for our model of the single-photon scheme the QBER in X- and Y- bases are the same and therefore we denote both by a single symbol e_{xy}.

A.6 SPADS and SPOTL schemes analysis

In order to compute the quantum bit error rate (QBER) of the Single-Photon with Additional Detection Setup (SPADS) scheme and the Single-Photon Over Two Links (SPOTL) scheme, we derive step by step the quantum state shared between Alice and Bob. The following results have been found using Mathematica. Finally, we also calculate the yield of the SPADS and SPOTL schemes.

Generation of elementary links

Single-photon scheme on Alice side

The application of the single-photon scheme on Alice's side leads Alice and the quantum repeater to share a state given in Eq. (A.53). This state can be rewritten as

$$\rho_{\text{A-QR}^e} = A_1 \left|\Psi^+\right\rangle\!\left\langle\Psi^+\right| + B_1 \left|\Psi^-\right\rangle\!\left\langle\Psi^-\right| + C_1 \left(|10\rangle\langle 10| + |01\rangle\langle 01|\right) + D_1 |11\rangle\langle 11| + E_1 |00\rangle\langle 00| \ , \tag{A.57}$$

with $A_1 = A(\theta_A, Y_A)$, $B_1 = B(\theta_A, Y_A)$, $C_1 = C(\theta_A, Y_A)$, $D_1 = D(\theta_A, Y_A)$ and $E_1 = E(\theta_A, Y_A)$. Here we have that

$$\begin{aligned}
A(\theta, Y) &= \frac{1}{Y} 2\cos^2(\theta)\sin^2(\theta)\eta(1-p_d)\left[(F_{\text{prep}}^2 + (1-F_{\text{prep}})^2)\lambda + 2F_{\text{prep}}(1-F_{\text{prep}})(1-\lambda)\right] \ , \\
B(\theta, Y) &= \frac{1}{Y} 2\cos^2(\theta)\sin^2(\theta)\eta(1-p_d)\left[(F_{\text{prep}}^2 + (1-F_{\text{prep}})^2)(1-\lambda) + 2F_{\text{prep}}(1-F_{\text{prep}})\lambda\right] \ , \\
C(\theta, Y) &= \frac{2}{Y}\cos^2(\theta)\sin^2(\theta)p_d(1-p_d)(1-\eta) \ , \\
D(\theta, Y) &= \frac{1}{Y}\cos^4(\theta)\left(2(1-\eta)\eta(1-p_d) + \eta^2(1-p_d) + 2(1-\eta)^2 p_d(1-p_d)\right) \ , \\
E(\theta, Y) &= \frac{2}{Y}\sin^4(\theta)p_d(1-p_d) \ .
\end{aligned} \tag{A.58}$$

In the above Y denotes the yield or the probability of success of the single-photon scheme and is given by Eq. (A.52). Subscript A indicates that in that expression for the yield and for each of the above defined coefficients we use $\theta = \theta_A$. Moreover, we have made here the following change of notation with respect to the Appendix A.5, $|\downarrow\rangle \to |0\rangle$ and $|\uparrow\rangle \to |1\rangle$.

SWAP gate in the middle node

In the next step a SWAP gate is applied in the middle node to transfer the electron state to the nuclear spin of the NV center. This causes a depolarizing noise of parameter $F_{\text{swap}} = F_g^2$ (see Appendix A.1). The resulting state can then be written as

$$\rho_{\text{A-QR}^C} = F_{\text{swap}}\rho_{\text{A-QR}^e} + (1 - F_{\text{swap}})\,\text{tr}_{\text{QR}}[\rho_{\text{A-QR}^e}] \otimes \frac{\mathbb{I}_{2,\text{QR}}}{2} \ . \tag{A.59}$$

The procedure on Bob's side

We now use the electron spin of the quantum repeater to generate the second quantum state. Here the procedures for the SPADS and SPOTL schemes diverge.

In the procedure for the SPADS scheme, the quantum repeater generates a spin-photon entangled state where the photonic qubit is encoded in the time-bin degree of freedom. Since the spin-photon

entangled state is imperfect, the electron and the photon share a state

$$\rho_{\mathrm{QR}^e-B} = F_{\mathrm{prep}} \left|\Psi^+\right\rangle\!\left\langle\Psi^+\right| + (1 - F_{\mathrm{prep}}) \left|\Psi^-\right\rangle\!\left\langle\Psi^-\right| \ . \tag{A.60}$$

Here we use the following labeling for time-bin encoded early and late mode of the photon: $|e\rangle = |1\rangle$, $|l\rangle = |0\rangle$. This photon is then sent towards Bob's detector. The lossy channel acts on such a time-bin encoded qubit as an erasure channel and so the quantum spin-photon state of the successful events in which the photonic qubit successfully arrives at the detector is unaffected by the lossy channel.

For the SPOTL scheme the repeater's electron spin and Bob's quantum memory generate a second state of the form given in Eq. (A.53). We can rewrite this state as

$$\rho_{\mathrm{QR}^e-B} = A_2 \left|\Psi^+\right\rangle\!\left\langle\Psi^+\right| + B_2 \left|\Psi^-\right\rangle\!\left\langle\Psi^-\right| + C_2 \left(|10\rangle\langle 10| + |01\rangle\langle 01|\right) + D_2 \,|11\rangle\langle 11| + E_2 \,|00\rangle\langle 00| \ , \tag{A.61}$$

with $A_2 = A(\theta_B, Y_B)$, $B_2 = B(\theta_B, Y_B)$, $C_2 = C(\theta_B, Y_B)$, $D_2 = D(\theta_B, Y_B)$ and $E_2 = E(\theta_B, Y_B)$.

Decoherence in the quantum memories

Decoherence of the carbon spin in the middle node can be modeled identically for both the SPADS and SPOTL scheme.

During the $n < n^*$ attempts to generate the state $\rho_{\mathrm{QR}^e\text{-B}}$, the carbon spin in the middle node holding half of the state $\rho_{\mathrm{A\text{-}QR}^C}$ will decohere. Using the decoherence model discussed in Appendix A.2, decoherence of the carbon spin will thus give us

$$\rho'_{\mathrm{A\text{-}QR}^C} = F_{T_1}(F_{T_2}\rho_{\mathrm{A\text{-}QR}^C} + (1-F_{T_2})(\mathbb{I}_2 \otimes Z)\rho_{\mathrm{A\text{-}QR}^C}(\mathbb{I}_2 \otimes Z)^\dagger) + (1-F_{T_1})\,\mathrm{tr}_{\mathrm{QR}}[\rho_{\mathrm{A\text{-}QR}^C}] \otimes \frac{\mathbb{I}_{2,\mathrm{QR}}}{2} \ . \tag{A.62}$$

For key generation, Alice (SPADS and SPOTL schemes) and Bob (SPOTL scheme) can actually measure their electron spin(s) immediately after the generation of spin photon entanglement, preventing the effect of decoherence on these qubit(s).

Noise due to measurements

Measurement of the qubits of Alice and Bob

In the SPADS scheme Alice performs a measurement on her electron spin immediately after each of the spin-photon entanglement generation events to prevent any decoherence with time of this qubit. This measurement causes an error modeled as a depolarizing channel of parameter F_m. Bob on the other hand performs a measurement on a photonic qubit that is encoded in the time-bin degree of freedom. His measurement utilises the squashin map so that we can model the noise arising from this measurement as a depolarising channel with parameter α_B as described in Appendix A.1. Hence the total state just before the Bell measurement is given by

$$\begin{aligned}\rho_{A-QR-B} &= F_m\alpha_B\rho'_{\mathrm{A\text{-}QR}^C} \otimes \rho_{\mathrm{QR}^e-B} + (1-F_m)\alpha_B \frac{\mathbb{I}_{2,A}}{2} \otimes \mathrm{tr}_A[\rho'_{\mathrm{A\text{-}QR}^C}] \otimes \rho_{\mathrm{QR}^e-B} \\ &+ (1-\alpha_B)F_m\rho'_{\mathrm{A\text{-}QR}^C} \otimes \mathrm{tr}_B[\rho_{\mathrm{QR}^e-B}] \otimes \frac{\mathbb{I}_{2,B}}{2} + (1-F_m)(1-\alpha_B)\,\mathrm{tr}_{AB}[\rho'_{\mathrm{A\text{-}QR}^C} \otimes \rho_{\mathrm{QR}^e-B}] \otimes \frac{\mathbb{I}_{4,AB}}{4} \ .\end{aligned} \tag{A.63}$$

For the SPOTL scheme, both Alice and Bob perform a measurement on their electron spins immediately after each of the spin-photon entanglement generation events. This measurement causes an error modeled

as a depolarizing channel of parameter F_m on each qubit, which means that after both Alice and Bob succeeded in performing the single-photon scheme with the repeater, the total, four-qubit state just before the Bell-measurement and including the noise of the measurements of Alice and Bob will be given by

$$\rho_{A-QR-B} = F_m^2 \rho'_{\text{A-QR}^C} \otimes \rho_{\text{QR}^e-B} + (1-F_m)F_m \left[\frac{\mathbb{I}_{2,A}}{2} \otimes \text{tr}_A[\rho'_{\text{A-QR}^C}] \otimes \rho_{\text{QR}^e-B} + \rho'_{\text{A-QR}^C} \otimes \text{tr}_B[\rho_{\text{QR}^e-B}] \otimes \frac{\mathbb{I}_{2,B}}{2} \right] \tag{A.64}$$
$$+ (1-F_m)^2 \,\text{tr}_{AB}[\rho'_{\text{A-QR}^C} \otimes \rho_{\text{QR}^e-B}] \otimes \frac{\mathbb{I}_{4,AB}}{4} \ .$$

Bell state measurement

Before the entanglement swapping, we have a total state ρ_{A-QR-B}. We now perform a Bell state measurement on the two qubits in the middle node. The error coming from this measurement is modeled by concatenation of depolarizing channels (see Appendix A.1) which means that the measurement is actually performed on

$$\rho_{\text{fin}} = F_g^2 F_m^2 \rho_{A-QR-B} + F_g^2(1-F_m^2)\,\text{tr}_{QR^e}[\rho_{A-QR-B}] \otimes \frac{\mathbb{I}_{2,QR^e}}{2} + (1-F_g^2)\,\text{tr}_{QR}[\rho_{A-QR-B}] \otimes \frac{\mathbb{I}_{4,QR}}{4} \ . \tag{A.65}$$

While $\rho'_{\text{A-QR}^C}$ is not Bell diagonal for the SPADS scheme, ρ_{QR^e-B} is, and so we find that taking into account the classical correction (which will be performed on the measured bit-value by Alice and Bob) the four cases corresponding to different measurement outcomes are equivalent. This means that if we model the correction to be applied to the quantum state rather than the classical bit, then the four post-measurement bipartite states shared between Alice and Bob are exactly the same.

For the SPOTL scheme, both $\rho'_{\text{A-QR}^C}$ and ρ_{QR^e-B} are not Bell diagonal which means that the resulting state of qubits of Alice and Bob after the Bell state measurement depends on the outcome of this Bell measurement and those four corresponding states are not equivalent under local unitary corrections. In fact, the two states corresponding to the $\Phi^\pm$ outcomes and the two states corresponding to the $\Psi^\pm$ outcomes are pairwise equivalent under local Pauli corrections. Hence, we will derive two different QBER corresponding to the following different resulting states shared between Alice and Bob,

$$\rho_{\Phi,AB} = (\mathbb{I}_A \otimes U_{\Phi^\pm,B})\,\text{Tr}_{QR}\left[\frac{(\mathbb{I}\otimes|\Phi^\pm\rangle\langle\Phi^\pm|\otimes\mathbb{I})\rho_{\text{fin}}(\mathbb{I}\otimes|\Phi^\pm\rangle\langle\Phi^\pm|\otimes\mathbb{I})^\dagger}{\text{Tr}(\rho_{\text{fin}}(\mathbb{I}\otimes|\Phi^\pm\rangle\langle\Phi^\pm|\otimes\mathbb{I}))} \right] (\mathbb{I}\otimes U_{\Phi^\pm,B})^\dagger \ , \tag{A.66}$$

$$\rho_{\Psi,AB} = (\mathbb{I}_A \otimes U_{\Psi^\pm,B})\,\text{Tr}_{QR}\left[\frac{(\mathbb{I}\otimes|\Psi^\pm\rangle\langle\Psi^\pm|\otimes\mathbb{I})\rho_{\text{fin}}(\mathbb{I}\otimes|\Psi^\pm\rangle\langle\Psi^\pm|\otimes\mathbb{I})^\dagger}{\text{Tr}(\rho_{\text{fin}}(\mathbb{I}\otimes|\Psi^\pm\rangle\langle\Psi^\pm|\otimes\mathbb{I}))} \right] (\mathbb{I}\otimes U_{\Psi^\pm,B})^\dagger \ . \tag{A.67}$$

Here $U_{\Phi^\pm,B}$ and $U_{\Psi^\pm,B}$ denote the four Pauli corrections implemented by Bob after the corresponding outcome of the Bell measurement. Note that for the SPADS scheme $\rho_{\Phi,AB} = \rho_{\Psi,AB}$.

The yield and QBER

A.6.0.1 Yield

For both SPADS and SPOTL scheme we calculate the yield as the inverse of the number of channel uses required to generate one bit of raw key, $Y = 1/\mathbb{E}[N]$, where $\mathbb{E}[N]$ is given by Eq. (A.31). For the SPOTL scheme in that formula we use $p_{A/B} = Y_{A/B}$, where $Y_{A/B}$ denotes the yield of the single-photon

scheme on Alice's/Bob's side given by Eq. (A.52). For the SPADS scheme p_A takes the same form as for the SPOTL scheme (but is now calculated for two thirds of the total distance between Alice and Bob rather than half), while p_B is the probability of registering a click in Bob's optical detection setup as in the SiSQuaRe scheme.

Extraction of the qubit error rates

By projecting these final corrected states onto the correct subspaces, we can obtain the qubit error rates e_z and e_{xy} (with our model we find that for both SPADS and SPOTL schemes the error rates in X and Y bases are the same). The state shared between Alice and Bob after the Pauli correction will always be the same for the SPADS scheme. Thus, there is only a single QBER e_z and e_{xy} independently of the outcome of the Bell measurement. For the SPOTL scheme that is not the case, there will be two set of QBER corresponding to the states $\rho_{\Phi,AB}$ and $\rho_{\Psi,AB}$.

$$e_{z,\Phi} = \mathrm{Tr}((|00\rangle\langle 00| + |11\rangle\langle 11|)\rho_\Phi) \ , \tag{A.68}$$

$$e_{z,\Psi} = \mathrm{Tr}((|00\rangle\langle 00| + |11\rangle\langle 11|)\rho_\Psi) \ , \tag{A.69}$$

$$e_{xy,\Phi} = \mathrm{Tr}((|+-\rangle\langle +-| + |-+\rangle\langle -+|)\rho_\Phi) = \mathrm{Tr}((|0_y1_y\rangle\langle 0_y1_y| + |1_y0_y\rangle\langle 1_y0_y|)\rho_\Phi) \ , \tag{A.70}$$

$$e_{xy,\Psi} = \mathrm{Tr}((|+-\rangle\langle +-| + |-+\rangle\langle -+|)\rho_\Psi) = \mathrm{Tr}((|0_y1_y\rangle\langle 0_y1_y| + |1_y0_y\rangle\langle 1_y0_y|)\rho_\Psi) \ . \tag{A.71}$$

Again, for the SPADS scheme $e_{z,\Phi} = e_{z,\Psi} = e_z$ and $e_{xy,\Phi} = e_{xy,\Psi} = e_{xy}$.

Averaging the qubit error rates

We have now derived the qubit error rates as a function of the experimental parameters. For the SPOTL scheme we now average the QBER over the two outcomes to get the final average QBER

$$\langle e_z \rangle = \langle p_\Psi e_{z,\Psi} + p_\Phi e_{z,\Phi} \rangle \ , \tag{A.72}$$

$$\langle e_{xy} \rangle = \langle p_\Psi e_{xy,\Psi} + p_\Phi e_{xy,\Phi} \rangle \ , \tag{A.73}$$

where p_Ψ (p_Φ) is the probability of measuring one of the $|\Psi\rangle$ ($|\Phi\rangle$) states in the Bell measurement and $\langle ... \rangle$ is found by averaging the expression over the number of Bob's attempts n with the geometric distribution within the first n^* trials. For the SPADS scheme $\langle e_z \rangle$ and $\langle e_{xy} \rangle$ can be averaged directly. The dependence on n arises from the decoherence terms F_{T_1} and F_{T_2}. Indeed, those terms correspond to the decoherence in the middle node during the attempts on Bob's side. Denoting by p_B the probability that in a single attempt Bob generates entanglement with the quantum repeater using the single-photon scheme for the SPOTL scheme and using direct transmission of the time-bin encoded qubit from the repeater to Bob for the SPADS scheme, we have that the exponentials in those expressions can be averaged as follows [23]

$$\langle e^{-cn} \rangle = \frac{p_B e^{-c}}{1-(1-p_B)^{n^*}} \frac{1-(1-p)^{n^*} e^{-cn^*}}{1-(1-p_B)e^{-c}} \ . \tag{A.74}$$

A.7 Secret-key fraction and advantage distillation

In this section we review the formulas for the secret-key fraction for the QKD protocols used in our model as a function of the QBER.

One-way BB84 protocol

For the fully asymmetric BB84 protocol with standard one-way post-processing, the secret-key fraction is given by [186, 188]:

$$r = 1 - h(e_x) - h(e_z) \ , \tag{A.75}$$

where $h(x)$ is the binary entropy function. Note that this formula is symmetric under the exchange of e_x and e_z - that is, the secret-key fraction is the same independently of whether we extract the key in the Z- or X-basis. As we will see later in this section, this is not the case for the six-state protocol with advantage distillation.

Six-state protocol with advantage distillation

Now we shall examine the six-state protocol with advantage distillation of [187]. For the purpose of this section, following the notation of [187], we shall denote the four Bell states as

$$|\psi(\mathsf{x},\mathsf{z})\rangle = \frac{1}{\sqrt{2}}(|0\rangle\,|0+\mathsf{x}\rangle + (-1)^{\mathsf{z}}\,|1\rangle\,|1+\mathsf{x}\ (\mathrm{mod}\,2)\rangle), \tag{A.76}$$

for $\mathsf{x},\mathsf{z} \in \{0,1\}$. We then write the Bell-diagonal state as

$$\rho_{AB} = \sum_{\mathsf{x},\mathsf{z}\in\{0,1\}} p_{\mathsf{xz}}\,|\psi(\mathsf{x},\mathsf{z})\rangle\,\langle\psi(\mathsf{x},\mathsf{z})| \ . \tag{A.77}$$

The considered advantage distillation protocol is described in [187]. It is shown there that if the key is extracted in the Z-basis, then the secret-key fraction for the fully asymmetric six-state protocol supplemented with this two-way post-processing technique is given by

$$r_{\text{six-state}} = \max\left[1 - H(P_{\mathsf{XZ}}) + \frac{P_{\bar{\mathsf{X}}}(1)}{2} h\left(\frac{p_{00}p_{10}+p_{01}p_{11}}{(p_{00}+p_{01})(p_{10}+p_{11})}\right), \frac{P_{\bar{\mathsf{X}}}(0)}{2}(1 - H(P'_{\mathsf{XZ}}))\right], \tag{A.78}$$

where

$$P_{\bar{\mathsf{X}}}(0) = (p_{00}+p_{01})^2 + (p_{10}+p_{11})^2 \ , \tag{A.79}$$

$$P_{\bar{\mathsf{X}}}(1) = 2(p_{00}+p_{01})(p_{10}+p_{11}) \ , \tag{A.80}$$

$$p'_{\mathsf{00}} = \frac{p_{00}^2+p_{01}^2}{(p_{00}+p_{01})^2+(p_{10}+p_{11})^2}, \tag{A.81}$$

$$p'_{\mathsf{10}} = \frac{2p_{00}p_{01}}{(p_{00}+p_{01})^2+(p_{10}+p_{11})^2}, \tag{A.82}$$

$$p'_{\mathsf{01}} = \frac{p_{10}^2+p_{11}^2}{(p_{00}+p_{01})^2+(p_{10}+p_{11})^2}, \tag{A.83}$$

$$p'_{\mathsf{11}} = \frac{2p_{10}p_{11}}{(p_{00}+p_{01})^2+(p_{10}+p_{11})^2} \ , \tag{A.84}$$

P_{XZ} (P'_{XZ}) is the probability distribution over the coefficients p_{xz} (p'_{xz}) and $H(P_{\mathsf{XZ}})$ ($H(P'_{\mathsf{XZ}})$) is the Shannon entropy of this distribution.

Now let us have a look at how to link the Bell coefficients p_{xz} with our QBER e_z and e_{xy} (for all our schemes the estimated QBER in the X-basis is the same as in the Y-basis). In this section we assume the target state that Alice and Bob want to generate to be $|\psi(\mathsf{0},\mathsf{0})\rangle$. Note that in the analysis in Appendices A.5 and A.6 it is the state $|\psi(\mathsf{1},\mathsf{0})\rangle$ that is a target, but of course the secret-key fraction analysis is independent of which Bell-state is a target state as they are all the same up to local Pauli rotations. Hence, the relation between the Bell-diagonal coefficients and the QBER is

$$p_{10} + p_{11} = e_z \ , \tag{A.85}$$

$$p_{01} + p_{11} = e_{xy} \ , \tag{A.86}$$

$$p_{01} + p_{10} = e_{xy} \ , \tag{A.87}$$

$$p_{00} + p_{01} + p_{10} + p_{11} = 1 \ . \tag{A.88}$$

Therefore

$$\begin{aligned} p_{00} &= 1 - \frac{e_z}{2} - e_{xy} \ , \\ p_{01} &= e_{xy} - \frac{e_z}{2} \ , \\ p_{10} &= p_{11} = \frac{e_z}{2} \ . \end{aligned} \tag{A.89}$$

And so

$$P_{\bar{\mathsf{X}}}(0) = 1 - 2e_z + 2e_z^2 \ , \tag{A.90}$$

$$P_{\bar{\mathsf{X}}}(1) = 2(1 - e_z)e_z \ . \tag{A.91}$$

It is important to note that for the above described advantage distillation, the amount of generated secret key depends on the basis in which it is extracted, as has been shown in [229]. Let us now have a look at the amount of key that can be extracted in the X- and Y-bases. As has been shown in [229], the secret-key fraction in these cases is also given by Eq. (A.78) but now the Bell coefficients depend on QBER in the following way:

$$\begin{aligned} p_{00} &= 1 - \frac{e_z}{2} - e_{xy} \ , \\ p_{10} &= e_{xy} - \frac{e_z}{2} \ , \\ p_{01} &= p_{11} = \frac{e_z}{2} \ . \end{aligned} \tag{A.92}$$

And so

$$\begin{aligned} P_{\bar{\mathsf{X}}}(0) &= 1 - 2e_{xy} + 2e_{xy}^2 \ , \\ P_{\bar{\mathsf{X}}}(1) &= 2(1 - e_{xy})e_{xy} \ . \end{aligned} \tag{A.93}$$

We note that we have assumed here that in the case of key extraction in Y-basis, either Alice or Bob applies a local bit flip in the Y-basis to the shared state, as the target state $|\psi(0,0)\rangle$ is anti-correlated in that basis.

In [229] it has been also observed that in the considered case of having the QBER in the X- and Y-bases being equal, the six-state protocol with advantage distillation allows us to extract more key if it is extracted in the basis with higher QBER. This observation determines the basis that we use for extracting key for the single-photon and the SPOTL schemes that use fully asymmetric six-state protocol with advantage distillation. Specifically, for the single-photon scheme we observe higher QBER in the Z-basis, while for the SPOTL scheme the QBER is higher in the X- and Y-bases. Therefore these are the bases that we choose to use for extracting key for those schemes.

For the SiSQuaRe and SPADS schemes the symmetric six-state protocol is used, hence for those schemes we group the raw bits into three groups corresponding to three different key-extraction bases and we extract the key separately for each of these bases. Finally, to obtain the final secret-key fraction, we note that for the symmetric six-state protocol we also need to include sifting, that is only one third of all the raw bits were obtained by Alice and Bob measuring in the same basis (the raw bits for the protocol runs in which they measured in different bases are discarded). Hence, if we denote by r_i the secret-key fraction obtained from the group of raw bits in which both Alice and Bob measured in the basis i, the final secret-key fraction for the six-state protocol for those schemes is given by

$$r = \frac{1}{3}\left(\frac{1}{3}r_x + \frac{1}{3}r_y + \frac{1}{3}r_z\right) . \tag{A.94}$$

Clearly in our case we have $r_x = r_y = r_{xy}$.

One-way six-state protocol

In Figure 4.7 we have also plotted the secret-key fraction for the one-way six-state protocol. For the fully asymmetric protocol and the case in which the key is extracted in the Z-basis, it is given by [186]

$$r = 1 - e_z h\left(\frac{1 + (e_x - e_y)/e_z}{2}\right) - (1 - e_z)h\left(\frac{1 - (e_x + e_y + e_z)/2}{1 - e_z}\right) - h(e_z) . \tag{A.95}$$

Although this formula does not appear to be symmetric under the permutation of e_x, e_y, e_z, it is in fact invariant under this permutation [230]. This means that for the symmetric one-way six-state protocol, in our case the final secret-key fraction is given by the expression in Eq. (A.95) multiplied by the sifting efficiency of one-third.

A.8 Runtime of the experiment

In this section we will detail how to perform an experiment that will be able to establish that a setup can surpass the capacity of a quantum channel modeling losses in a fiber (see Eq. (4.5)). This experiment can validate a setup to qualify as a quantum repeater, without explicitly having to generate secret-key. We show then that, for the listed parameters in the main text, the single-photon scheme can be certified to be a quantum repeater within approximately twelve hours.

The experiment is based on estimating the yield of the scheme and the individual QBER of the generated states. More specifically, here we will calculate the probability that, assuming our model is accurate and each individual run is independent and identically distributed, the observed estimate of the yield and the individual QBER are larger and smaller, respectively, than some fixed threshold values. If, with these threshold values for the yield and QBER, the calculated asymptotic secret-key still surpasses the capacity, we can claim a working quantum repeater. The experiment consists of first performing n attempts at generating a state between Alice and Bob, from which the yield can be estimated by calculating the ratio of the successful attempts and n. Then, the QBER in each basis is estimated by Alice and Bob measuring in the same basis in each of the successful attempts.

Central to our calculation is the fact that, for n instances of a Bernoulli random variable with probability p, the probability that the number of observed successes $S(n)$ is smaller or equal than some value k is equal to

$$P\left(S(n) \leq k\right) = \sum_{i=0}^{k} \binom{n}{i} p^i \left(1-p\right)^{n-i} \ . \tag{A.96}$$

Assuming the outcomes of our experiment are independent and identically distributed, the observed yield $\bar{Y}$ satisfies

$$P\left(\bar{Y} \leq \left(Y - t_Y\right)\right) = P\left(n\bar{Y} \leq n\left(Y - t_Y\right)\right) = \sum_{i=0}^{\lfloor n(Y-t_Y)\rfloor} \binom{n}{i} Y^i \left(1-Y\right)^{n-i} \ , \tag{A.97}$$

where $Y - t_Y$ is the lower threshold. Let us make this more concrete with a specific calculation. For a distance of $17L_0$ the yield is equal to $\approx 5.6 \cdot 10^{-6}$. Setting the maximum deviation in the yield to $\bar{Y} = Y - t_Y$ with $t_Y = 2.0 \cdot 10^{-7}$ and the number of attempts to $n = 5 \cdot 10^9$ (which corresponds to approximately a runtime of twelve hours assuming a single attempt takes $8.5 \cdot 10^{-6}$ s, corresponding to t_{prep} and a single-shot readout lasting $2.5 \cdot 10^{-6}$ s), we find that

$$P\left(\bar{Y} \leq \left(Y - t_Y\right)\right) \leq 9.2 \cdot 10^{-10} \ . \tag{A.98}$$

Similarly, for the individual errors $\{e_k\}_{k\in\{x,y,z\}}$ in the three bases we have that

$$P\left(\bar{e}_k \geq \left(e_k + t_k\right)\right) = P\left(m \cdot \bar{e}_k \geq m\left(e_k + t_k\right)\right) = \sum_{i=\lceil m(e_k+t_k)\rceil}^{m} \binom{m}{i} \left(e_k\right)^i \left(1-e_k\right)^{m-i} \ . \tag{A.99}$$

Here we set $m = \left\lfloor \frac{n}{3}\left(Y - t_Y\right)\right\rfloor$, which is an estimate for the number of raw bits that Alice and Bob obtain from measurements in each of the three bases, for the total n attempts of the protocol. All the

raw bits from those three sets are then compared to estimate the QBER in each of the three bases. Note that we gather the same amount of samples for each basis, even when an asymmetric protocol would be performed. Setting $t_i = t = 0.015,\ \forall i \in \{x, y, z\}$ and, as before, $n = 5 \cdot 10^9$, we find, at a distance of $17L_0$ where $e_z \approx 0.171$ and $e_y = e_x \approx 0.141$, that

$$P\left(\bar{e}_z \geq (e_z + t)\right) \leq 9.0 \cdot 10^{-5} \ , \tag{A.100}$$

$$P\left(\bar{e}_y \geq (e_y + t)\right) = P\left(\bar{e}_x \geq (e_x + t)\right) \leq 2.7 \cdot 10^{-5} \ . \tag{A.101}$$

Then, with probability at least

$$\begin{aligned} &\left(1 - P\left(\bar{e}_x \geq (e_x + t)\right)\right) \cdot \left(1 - P\left(\bar{e}_y \geq (e_y + t)\right)\right) \cdot \left(1 - P\left(\bar{e}_z \geq (e_z + t)\right)\right) \cdot \left(1 - P\left(\bar{Y} \leq (Y - t_Y)\right)\right) \qquad \text{(A.102)} \\ &\geq 1 - 1.5 \cdot 10^{-4} \ , \qquad \text{(A.103)} \end{aligned}$$

none of the observed QBER and yield exceed their threshold conditions. The corresponding lowest secret-key rate for these parameters (with a yield of $Y - t_Y$ and QBER of $e_x + t_x,\ e_y + t_y,\ e_z + t_z$) is $\approx 1.97 \cdot 10^{-7}$, which we observe is greater than the secret-key capacity by a factor ≈ 3.29 (see Eq.(4.5)) at a distance of $17L_0$, since the secret-key capacity equals $-\log_2\left(1 - e^{-17}\right) \lesssim 5.97 \cdot 10^{-8}$.

Thus, with high probability we can establish that the single-photon scheme achieves a secret-key rate significantly greater than the corresponding secret-key capacity for a distance of $17L_0 \approx 9.2$ kilometer within approximately twelve hours.

A.9 MDI QKD

We note here that the single-photon scheme for generating key is closely linked to the measurement device independent (MDI) QKD protocol [231]. In particular it is an entanglement-based version of a scheme in which Alice and Bob prepare and send specific photonic qubit states to the heralding station in the middle, where the qubits are encoded in the presence/absence of the photon. We note that in the ideal case of the single-photon scheme, the spin-photon state is given in Eq. (A.35). For the six-state protocol the spin part of this state is then measured in the X-, Y- or Z- basis at random according to a fixed probability distribution (this probability distribution dictates whether we use symmetric or asymmetric protocol). Considering the probabilities of the individual measurement outcomes, this is equivalent to the scenario in which Alice and Bob choose one of the three set of states at random according to the same probability distribution and prepare each of the two states from that set with the probability equal to the corresponding measurement outcome probability. These sets do not form bases, as the two states within each set are not orthogonal. We will therefore refer to these sets here as "pseudo-bases". Depending on the chosen pseudo-basis they prepare one of the six states encoding the bit value of "0" or "1" in that pseudo-basis. These states and the corresponding preparation probabilities are

- pseudo-basis 1: $\{|0\rangle, |1\rangle\}$ with probabilities $\{\sin^2\theta,\ \cos^2\theta\}$,
- pseudo-basis 2: $\{\sin\theta\,|0\rangle + \cos\theta\,|1\rangle,\ \sin\theta\,|0\rangle - \cos\theta\,|1\rangle\}$ with probabilities $\{\frac{1}{2}, \frac{1}{2}\}$,
- pseudo-basis 3: $\{\sin\theta\,|0\rangle + i\cos\theta\,|1\rangle,\ \sin\theta\,|0\rangle - i\cos\theta\,|1\rangle\}$ with probabilities $\{\frac{1}{2}, \frac{1}{2}\}$.

These states are then sent towards the beam splitter station. The station performs the standard photonic Bell-state measurement and sends the outcome to both Alice and Bob. Alice and Bob discard all the runs for which the beam splitter station measured A_2 (recall the measurement operators in Eq. (A.44)). They then exchange the classical information about their pseudo-basis choice and keep only the data for the runs in which they both used the same basis. For those data they apply the following post-processing in order to obtain correlated raw bits

- pseudo-basis 1: for both outcomes A_0 and A_1 Bob flips the value of his bit.
- pseudo-basis 2: for the outcome A_0 they do nothing, for the outcome A_1 Bob flips the value of his bit.
- pseudo-basis 3: for the outcome A_0 they do nothing, for the outcome A_1 Bob flips the value of his bit.

In this way Alice and Bob have generated their strings of raw bits.

We note here that the direct preparation of the six states from the three pseudo-bases described above in the photonic presence/absence degree of freedom is experimentally hard. This is related to the fact that linear optics does not allow to easily perform single qubit rotations necessary to prepare these states. The use of memory-based NV-centers offers a great advantage here, as in these schemes the rotations that allow us to obtain the required amplitudes of the photonic states are performed on the electron spins rather than the photons themselves. There has also been proposed an alternative scheme that also benefits from single photon detection events in which Alice and Bob send coherent pulses to the heralding station [232, 163].

APPENDIX B

Appendix: Documentation for the Netsquid library

In this thesis, particularly in Chapters 5 and 6 we have simulated metropolitan networks linked with satellite links. These simulations have been done using Netsquid [202, 31], a python-based discrete event network simulator developped in QuTech (Delft) on top of which we have built our own functions for the functionalities we needed. In this appendix we give a documentation for these functions.

B.1 Qlient, Qonnector and Network initialisation

Our Quantum City model is based on two types of nodes: Qlients (end users) and Qonnector (servers giving access to quantum-enhanced functionalities). In our code they are modeled with two classes, subclasses of the Node class, itself a subclass of the Netsquid Component class (see Fig. B.1). They contain the classical empty slots that we will use to store measurement outputs during protocols or to create connections between the different nodes of our network.

More specifically each **Qlient** has a *keylist* attribute where it will store raw key bits as well as a *listport* attribute to make the connections easy during the protocol runs. When a Qlient node is created, it automatically generates a Quantum Processor of size 1 to be able to process single qubits.

Qonnectors also have a *QlientPort* attribute to help with the connections, a *QlientList* attribute to store the name of each Qlient it is attached to and a *QlientKeys* attribute to store raw key bits for each Qlient. Qonnector do not have a built-in quantum processor but they will generate one for each Qlient they are connected to.

The network is initiated with the **QEurope** class. It has three methods allowing to add Qonnectors, to add Qlients or to connect Qonnectors via satellites or drones. The method adding a Qonnector simply creates a Qonnector node. The method adding a Qlient takes 3 arguments: the name of the Qlient, the Qonnector it should be attached to and the distance between the Qonnector and this Qlient. When the add_Qlient method is called, it creates a Qlient node and a Quantum processor is created at the Qonnector associated. It also creates two ways quantum and classical channels between the Qonnector and the Qlient. This means that for each Qlient, the Qonnector will have a separate processor.

```
124 class Qlient_node(Node):
125     """A Qlient node
126 
127     Parameters:
128     name: name of the Qlient
129     phys_instruction: list of physical instructions for the Qlient
130     keylist: list of bits for QKD
131     ports: list of two ports: one to send to Qonnector and one to receive
132     """
133 
134     def __init__(self, name, phys_instruction, keylist=None,listports=None):
135         super().__init__(name=name)
136         qmem = QuantumProcessor("QlientMemory{}".format(name), num_positions=1,
137                                 phys_instructions=phys_instruction)
138         self.qmemory = qmem
139         self.keylist=keylist
140         self.listports=listports
141 
142 class Qonnector_node(Node):
143     """A Qonnector node
144 
145     Parameters:
146     QlientList: List of connected Qlients
147     QlientPorts: Dictionnary of the form {Qlient: [port_to_send, port_to_receive]}
148     QlientKeys : Dictionnary for QKD of the form {Qlient: [key]}
149     """
150 
151     def __init__(self, name,QlientList=None,
152                  QlientPorts=None,QlientKeys=None):
153         super().__init__(name=name)
154         self.QlientList = QlientList
155         self.QlientPorts = QlientPorts
156         self.QlientKeys = QlientKeys
```

Figure B.1: Code for the Qlient and Qonnector classes

This facilitates simulations because in Netsquid, each processor has input and output ports that can be connected to one quantum channel only. It is when adding these connections that the list of port attribute of the Qonnector and Qlient classes are useful. The quantum channel between a Qlient and the Qonnector is associated with a Fiber noise model that already exists in Netsquid.

Finally the Connect_Qonnector method of the QEurope class connects two Qonnectors via a free-space channel, either directly or via a satellite. It takes as arguments the name of the two Qonnectors that should be connected, the distance between them or between each of them and the satellite, the atmospheric transmittance and the link type: 'satellite' or 'drone'. When 'satellite' is selected, it creates a new Qonnector called Satellite at a distance specified by the parameters of the method. In this case the connect_qonnector function takes as input the name of the two Qonnectors, the length of the two links between each Qonnector and the satellite and the atmospheric transmittance of each link. When 'drone' is selected, it creates two qonnector nodes called DroneQonnector1 and DroneQonnector2 and a link between them as well as a link to each qonnector. The parameters here are the name of the two Qonnectors, the height of the drone, the distance between the drones, the atmospheric transmittance between the drones and the atmospheric transmittance between the drones and the ground. The noise model of these quantum channels have been created in collaboration with researchers of the LIP6 QI team: Matteo Schiavon and Valentina Marulanda Acosta.

The node parameters such as the time it takes to create a pair or the probability of success can be changed at will in the main QEurope file to match a particular simulation. Satellites are initialized using the *create_satellite* python file which uses the orekit package and the *channel* file to get the elevation, the distance to the ground stations and atmospheric transmittance depending on the atmospheric model that is chosen. This creates an *npz* file that can be used to simulate the orbit of a satellite.

To summarise, a network is first initiated by calling the QEurope class and then by adding Qonnectors and Qlients with the methods of the class (see Fig. B.2).

```
#Creation of a European network instance
net2 = QEurope("Europe")

#Quantum City in Paris
net2.Add_Qonnector("QonnectorParis")
net2.Add_Qlient("Jussieu",0.001,"QonnectorParis")
net2.Add_Qlient("IRIF",3.01,"QonnectorParis")
net2.Add_Qlient("Telecom",18.77,"QonnectorParis")
net2.Add_Qlient("Chatillon",6.77,"QonnectorParis")
net2.Add_Qlient("CEA",31.35,"QonnectorParis")

#Quantum City in the Netherland
net2.Add_Qonnector("QonnectorNetherland")
net2.Add_Qlient("Rotterdam", 12.62,"QonnectorNetherland")
net2.Add_Qlient("QuSoft Amsterdam",54.72,"QonnectorNetherland")

#Connection of the two quantum cities via satellite
net2.Connect_Qonnector("QonnectorParis","QonnectorNetherland", lenSatParis[i]/1000, lenSatDelft[i]/1000,
                       tSatParis[i], tSatDelft[i], "satellite")
```

Figure B.2: Example of the creation of a Network with two Quantum cities linked by a Satellite. the parameters in the Connect_Qonnector method are given by the satellite data *npz* file and depend on the position i of the satellite.

B.2 Protocols

We now explain the different protocols that we implemented in this model. They are all subclasses of the NodeProtocol Netsquid class which allows the simulation of discrete events for a given simulation time. Protocols are virtual simulation entities that are attached to components such as our Qlient node to steer their behaviour. This means that calling a protocol on a node will drive the components such as the quantum processors embedded in that node.

- The **SendBB84** node protocol creates and sends random BB84 states. It takes as argument the success probability p_{init} and the flip probability p_{flip} for creating a single photon (see Sec. 5.1.2) as well as the node it should send the qubit to. The protocol first creates a clock that gives him the timesteps that depend on the initialisation time given as parameter to the program. After flipping a coin following a Bernouilli distribution with success probability p_{init} at each timestep, it will create a $|0\rangle$ state and store it in the processor of the node. It will then flip it with probability p_{flip} by applying an X operation on it. If the state is created, a random bit and a random basis is then chosen and the appropriated operations is performed on the $|0\rangle$ state to transform it in either $|0\rangle, |1\rangle, |+\rangle$ or $|-\rangle$. The bit and basis chosen are recorded in the key list attribute of the node. The 'pop' method is then called on the quantum processor which will automatically send the qubit out of the memory, through the output port and the quantum channel linked to it. The timestamp associated with the qubit is sent at the same time via the classical channel. We assume for simplifying the simulation that information travelling in both quantum and classical channels travel at the same speed and that it takes 1ns to go from any node to another.
- The **ReceiveProtocol** node protocol is performed by a node to receive a state a measure it. It saves the outputs as well as the measurement basis and timestamps of reception in the list QlientKeys["name of the sending node"] in the case of a Qonnector or in the list keylist in the

case of a Qlient. It takes as input the name of the node from which qubits are expected, the probability that the measurement succeeds $meas_{succ}$ or flips the outcome $meas_{flip}$ and a boolean BB84 indicating if the measurement basis should be randomized. When this protocol is called on a node, the receiving port of the node will await for qubits until the end of the simulation time. Whenever a qubit arrives, it is stored in the quantum processor of the node. If BB84 is False then the measurement is always done in the computational basis, otherwise a random base is chosen. After flipping coins to decide whether to actually perform the measurement or to apply an X operation on the qubit, it will measure the qubit in the appropriate basis and store the output and the measurement basis. At the same time it will receive the classical timestamp on the classical channel and store it along with the output.

- The **TransmitProtocol** node protocol is used by a Qonnector to transmit a qubit sent by a Qlient or a satellite to another Qlient. It takes as input a node from which to expect qubit, another to send qubits to and a success probability $switch_{succ}$. When this method is called on a node, it will open its quantum ports and wait for the reception of a qubit. Whenever this happens, it flips a coin with probability $switch_{succ}$. If the outcome is positive, it moves the qubit from the processor associated to the node that sent a qubit to the processor associated with the node that should receive the qubit. It also transmit the classical timestamp associated if there is one.
- The **SendEPR** node protocol is performed by a Qonnector or a satellite node to create and send an EPR pair to two nodes, each getting one qubit. It takes as input the two nodes it should send the qubits to and a success probability EPR_{succ}. It creates a QSource component that creates EPR pairs at a rate given by the parameters of the program and with probability of success EPR_{succ}. The qubits from the EPR pairs are then given to the processors associated with the node that should receive the qubits. A simple call to the 'pop' function on these processors automatically sends the qubit to the receiving nodes. A classical signal indicating the timestamp of each qubit sending is also going to the receiving node. To keep track of how many pairs are actually sent by the node, a '0' is stored in the memory of the node.
- The **BSMProtocol** node protocol corresponds to a Bell state measurement performed by a Qonnector node on two qubits received from two different Qlients simultaneously. It takes as input the two Qlient from wich the qubits are expected and a probability that the Bell state measurement succeeds BSM_{succ}. It can only be performed by a Qonnector node and the outputs are stored in the *QlientKeys['name of the Qlients']* attribute. When this protocol is called by a Qonnector node, it will open its input ports and whenever qubits are in the two processors associated to the two Qlients, it does a comparison of the timestamp received with them. If they are equal, it then moves one qubit in the other qubit's processor and perform a CNOT gate on the two qubits, then a Hadamard gate on the first one and finally measure the two qubits with success probability BSM_{succ}. This implements a Bell State measurement.
- The **SendGHZ3**, **SendGHZ4** and **SendGHZ5** node protocols work in the same way as the SendEPR protocol to create and send GHZ states to 3, 4 or 5 Qlients. They take as input the name of the Qlients and the success probability GHZ_{succ}.

As an example we show below in Fig. B.3 the code following the one of Fig. B.2 to send an EPR pair from the satellite to two Qonnectors used as ground stations, who in turn transmit the qubits to two Qlients who receive and measure it.

```
net = net2.network
Satellite = net.get_node("SatelliteQonnectorParisQonnectorNetherland")
Paris = net.get_node("QonnectorParis")
Delft =net.get_node("QonnectorNetherland")
Bob = net.get_node("IRIF")
Hadi = net.get_node("Rotterdam")

#Initialisation of the classical memory to store the keys
Paris.QlientKeys[Satellite.name] = []
Delft.QlientKeys[Satellite.name] = []
Satellite.QlientKeys[Paris.name] = []
Satellite.QlientKeys[Delft.name] = []
Bob.keylist = []
Hadi.keylist = []

#protocol to send EPR pairs from the satellite at a rate f_EPR and with success probability EPR_succ
ProtocolS = SendEPR(Paris, Delft, EPR_succ, Satellite)
ProtocolS.start()

#Transmission to the Qlients
protocolS1 = TransmitProtocol(Satellite, Bob, switch_succ, Paris)
protocolS1.start()
protocolS2 = TransmitProtocol(Satellite, Hadi, switch_succ, Delft)
protocolS2.start()

#Protocol to receive photons with success probability Qonnector_meas_succ and flipping probability Qonnector_meas_flip.
#This protocol measure randomly the arriving photon in the X or Z basis and stor the output in list QlientKey of the qonnectors
protocolA = ReceiveProtocol(Paris, Qonnector_meas_succ, Qonnector_meas_flip,False, Bob)
protocolA.start()

protocolB = ReceiveProtocol(Delft, Qonnector_meas_succ, Qonnector_meas_flip,False, Hadi)
protocolB.start()
stat =ns.sim_run(duration=simtime)
```

Figure B.3: Example code for creating a raw key between two Qlients in two different Cities using entanglement-based QKD with a satellite as a source of EPR pairs. The last command *sim_run* starts the simulation for some time *simtime*.

B.3 Classical Post Processing

We also defined a few functions to extract relevant data from the outcomes of the protocols. After a protocol is done, the nodes that were involved hold in their classical memory slots the outcome of measurements. Each outcome is recorded alongside with its timestamp and its measurement basis. We added **Sifting** functions taking as input two, three, four or five raw outcome lists and outputing a single list with the outcomes that have the same timestamp. This resulting sifted list contains tuples where each element of the tuple corresponds to the output of one of the parties involved.

From the sifted list we can compute the final raw sifted key rate and throughput by dividing its length by the number of qubits sent or by the time of the simulation. We can also extract the Qubit Error Rate (QBER) with the functions **estimQBER, estimQBERGHZ3, estimQBERGHZ4** and **estimQBERGHZ5**. These functions will simply look at the tuple in the sifted list, count the non-matching outcomes and divide it by the length of the sifted list. We also added the **estimQBEREPR** function that does the same job but this time counting the matching outcomes since the BBM92 protocol uses the Bell state $|\psi^-\rangle$ which creates perfectly unmatched bits.

Finally the dark counts are added directly on the outcome list with the function **addDarkCounts**. It takes as a parameter a list of outcomes, the probability that a dark count happens p_{dark} and the last timestep of the protocol. For each timestep it will either add a random outcome to the list if there is none or remove an outcome if there is one with probability p_{dark}. The reason for the dark count to be added classically after the protocol is that the ReceiveProtocol records outcomes only when qubits arrive to the node. If they are lost before, nothing is added to the outcome list hence we could not directly add a probability that a random outcome appears. The addDarkCounts function thus have to be added to the resulting outcome lists if one wants to take into account background noise or cross-talk effects at the

detector.

Below we show in Fig. B.4 the code following the ones from the previous figures to add dark count and extract relevant data from the lists of measurement outcome.

```
stat =ns.sim_run(duration=simtime)

#Adding dark counts
addDarkCounts(Bob.keylist, pdarkbest, int(simtime/Qonnector_init_time))
addDarkCounts(Hadi.keylist, pdarkbest, int(simtime/Qonnector_init_time))

#Sifting: we only keep the qubit Bob and Hadi received from the same pair
L = Sifting(Bob.keylist,Hadi.keylist)

#List to get the number of EPR sent from the satellite
Lin= Satellite.QlientKeys[Paris.name]

print("Number of EPR sent : "+ str(len(Lin)))
print("Number of successful EPR transmission : " + str(len(L)))
print("Rate : " + str(len(L)/(simtime*1e9)))
print("Throughput : " + str(len(L)/len(Lin)))
print("QBER : "+ str(estimQBEREPR(L)))
```

Figure B.4: Example code for adding dark count and extract data from the protocol initiated in Fig. B.3.

Bibliography

[1] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition*.
Cambridge University Press, 2010.

[2] J. S. Bell, "On the einstein podolsky rosen paradox," *Physics Physique Fizika*, vol. 1, pp. 195–200, Nov 1964.

[3] B. Hensen, H. Bernien, A. Dréau, A. Reiserer, N. Kalb, M. Blok, J. Ruitenberg, R. Vermeulen, R. Schouten, C. Abellan, W. Amaya, V. Pruneri, M. Mitchell, M. Markham, D. Twitchen, D. Elkouss, S. Wehner, T. Taminiau, and R. Hanson, "Loophole-free bell inequality violation using electron spins separated by 1.3 kilometres," *Nature*, vol. 526, 10 2015.

[4] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, "Quantum entanglement," *Reviews of Modern Physics*, vol. 81, pp. 865–942, jun 2009.

[5] D. M. Greenberger, M. A. Horne, and A. Zeilinger, *Going Beyond Bell's Theorem*, pp. 69–72.
Dordrecht: Springer Netherlands, 1989.

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

[7] S. Bartolucci, P. Birchall, H. Bombin, H. Cable, C. Dawson, M. Gimeno-Segovia, E. Johnston, K. Kieling, N. Nickerson, M. Pant, F. Pastawski, T. Rudolph, and C. Sparrow, "Fusion-based quantum computation," 2021.

[8] L. Robledo, L. Childress, H. Bernien, B. Hensen, P. F. A. Alkemade, and R. Hanson, "High-fidelity projective read-out of a solid-state spin quantum register," *Nature*, vol. 477, no. 7366, pp. 574–578, 2011.

[9] P. C. Maurer, G. Kucsko, C. Latta, L. Jiang, N. Y. Yao, S. D. Bennett, F. Pastawski, D. Hunger, N. Chisholm, M. Markham, *et al.*, "Room-temperature quantum bit memory exceeding one second," *Science*, vol. 336, no. 6086, pp. 1283–1286, 2012.

[10] N. Kalb, A. A. Reiserer, P. C. Humphreys, J. J. Bakermans, S. J. Kamerling, N. H. Nickerson, S. C. Benjamin, D. J. Twitchen, M. Markham, and R. Hanson, "Entanglement distillation between solid-state quantum network nodes," *Science*, vol. 356, no. 6341, pp. 928–932, 2017.

[11] M. H. Abobeih, J. Cramer, M. A. Bakker, N. Kalb, M. Markham, D. J. Twitchen, and T. H. Taminiau, "One-second coherence for a single electron spin coupled to a multi-qubit nuclear-spin environment," *Nature Communications*, vol. 9, no. 1, p. 2552, 2018.

[12] L. J. Rogers, K. D. Jahnke, M. H. Metsch, A. Sipahigil, J. M. Binder, T. Teraji, H. Sumiya, J. Isoya, M. D. Lukin, P. Hemmer, and F. Jelezko, "All-optical initialization, readout, and coherent preparation of single silicon-vacancy spins in diamond," *Phys. Rev. Lett.*, vol. 113, p. 263602, Dec 2014.

[13] R. Mouktik, S. Chen, C. M. Phenicie, R. Ourari, A. M. Dibos, and J. D. Thompson, "Optical quantum nondemolition measurement of a single rare earth ion qubit," *Nature Communications*, vol. 11, p. 1605, mar 2020.

[14] H. C. Nägerl, D. Leibfried, H. Rohde, G. Thalhammer, J. Eschner, F. Schmidt-Kaler, and R. Blatt, "Laser addressing of individual ions in a linear ion trap," *Phys. Rev. A*, vol. 60, pp. 145–148, Jul 1999.

[15] S. D. Barrett, P. P. Rohde, and T. M. Stace, "Scalable quantum computing with atomic ensembles," *New Journal of Physics*, vol. 12, p. 093032, sep 2010.

[16] A. Dantan, N. Treps, A. Bramati, and M. Pinard, "Teleportation of an atomic ensemble quantum state," *Physical Review Letters*, vol. 94, feb 2005.

[17] J. R. Petta, A. C. Johnson, J. M. Taylor, E. A. Laird, A. Yacoby, M. D. Lukin, C. M. Marcus, M. P. Hanson, and A. C. Gossard, "Coherent manipulation of coupled electron spins in semiconductor quantum dots," *Science*, vol. 309, no. 5744, pp. 2180–2184, 2005.

[18] A. Chatterjee, P. Stevenson, S. D. Franceschi, A. Morello, N. P. de Leon, and F. Kuemmeth, "Semiconductor qubits in practice," *Nature Reviews Physics*, vol. 3, pp. 157–177, feb 2021.

[19] J. M. Martinis and K. Osborne, "Superconducting qubits and the physics of josephson junctions," 2004.

[20] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Journal on Computing*, vol. 26, pp. 1484–1509, oct 1997.

[21] Y. Ma, H. Miao, B. H. Pang, M. Evans, C. Zhao, J. Harms, R. Schnabel, and Y. Chen, "Proposal for gravitational-wave detection beyond the standard quantum limit through EPR entanglement," *Nature Physics*, vol. 13, pp. 776–780, may 2017.

[22] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, "Fundamental limits of repeaterless quantum communications," *Nature Communications*, vol. 8, apr 2017.

[23] F. Rozpędek, K. D. Goodenough, J. Ribeiro, N. Kalb, V. C. Vivoli, A. Reiserer, R. Hanson, S. Wehner, and D. Elkouss, "Parameter regimes for a single sequential quantum repeater," *Quantum Science and Technology*, vol. 3, p. 034002, 2018.

[24] K. Azuma, K. Tamaki, and H.-K. Lo, "All-photonic quantum repeaters," *Nature Communications*, vol. 6, apr 2015.

[25] S. DiAdamo, B. Qi, G. Miller, R. Kompella, and A. Shabani, "Packet switching in quantum networks: A path to quantum internet," 2022.

[26] "Quantum internet alliance, https://quantum-internet.team/."

[27] S. Wehner, D. Elkouss, and R. Hanson, "Quantum internet: A vision for the road ahead," *Science*, vol. 362, no. 6412, 2018.

[28] A. Dahlberg, M. Skrzypczyk, and S. Wehner, "The Link Layer service in a Quantum Internet," Internet-Draft draft-dahlberg-ll-quantum-03, Internet Engineering Task Force, Oct. 2019. Work in Progress.

[29] C. Meignant, D. Markham, and F. Grosshans, "Distributing graph states over arbitrary quantum networks," *Physical Review A*, vol. 100, nov 2019.

[30] A. Dahlberg, J. Helsen, and S. Wehner, "How to transform graph states using single-qubit operations: computational complexity and algorithms," 2018.

[31] T. Coopmans, R. Knegjens, A. Dahlberg, D. Maier, L. Nijsten, J. Oliveira, M. Papendrecht, J. Rabbie, F. Rozpedek, M. Skrzypczyk, L. Wubben, W. de Jong, D. Podareanu, A. T. Knoop, D. Elkouss, and S. Wehner, "Netsquid, a discrete-event simulation platform for quantum networks," 2021.

[32] R. Satoh, M. Hajdušek, N. Benchasattabuse, S. Nagayama, K. Teramoto, T. Matsuo, S. A. Metwalli, T. Satoh, S. Suzuki, and R. Van Meter, "Quisp: a quantum internet simulation package," 2021.

[33] A. Dahlberg and S. Wehner, "SimulaQron—a simulator for developing quantum internet software," *Quantum Science and Technology*, vol. 4, p. 015001, sep 2018.

[34] C. Greganti, P. Schiansky, I. A. Calafell, L. M. Procopio, L. A. Rozema, and P. Walther, "Tuning single-photon sources for telecom multi-photon experiments," *Opt. Express*, vol. 26, pp. 3286–3302, Feb 2018.

[35] N. Bruno, A. Martin, T. Guerreiro, B. Sanguinetti, and R. T. Thew, "Pulsed source of spectrally uncorrelated and indistinguishable photons at telecom wavelengths," *Optics express*, vol. 22, no. 14, pp. 17246–17253, 2014.

[36] D. Istrati, Y. Pilnyak, L. Cohen, H. S. Eisenberg, C. Anton-Solanas, J. C. L. Rosillo, P. Hilaire, H. Ollivier, C. Millet, A. Lemaítre, I. Sagnes, A. Harouri, L. Lanco, and P. Senellart, "Generating multi-photon entangled states from a single deterministic single-photon source," in *Quantum Information and Measurement (QIM) V: Quantum Technologies*, p. T3B.1, Optical Society of America, 2019.

[37] V. R. R. Valivarthi, M. Grimau, Q. Zhou, G. Aguilar, V. Verma, F. Marsili, M. Shaw, S. Nam, D. Oblak, and W. Tittel, "Quantum teleportation across a metropolitan fibre network," *Nature Photonics*, vol. 10, 09 2016.

[38] S.-K. Liao, W.-Q. Cai, J. Handsteiner, B. Liu, J. Yin, L. Zhang, D. Rauch, M. Fink, J.-G. Ren, W.-Y. Liu, Y. Li, Q. Shen, Y. Cao, F.-Z. Li, J.-F. Wang, Y.-M. Huang, L. Deng, T. Xi, L. Ma, T. Hu, L. Li, N.-L. Liu, F. Koidl, P. Wang, Y.-A. Chen, X.-B. Wang, M. Steindorfer, G. Kirchner, C.-Y. Lu, R. Shu, R. Ursin, T. Scheidl, C.-Z. Peng, J.-Y. Wang, A. Zeilinger, and J.-W. Pan, "Satellite-relayed intercontinental quantum network," *Phys. Rev. Lett.*, vol. 120, p. 030501, Jan 2018.

[39] J. Yin, Y. Cao, Y.-H. Li, S.-K. Liao, L. Zhang, J.-G. Ren, W.-Q. Cai, W.-Y. Liu, B. Li, H. Dai, *et al.*, "Satellite-based entanglement distribution over 1200 kilometers," *Science*, vol. 356, no. 6343, pp. 1140–1144, 2017.

[40] J. Yin, Y.-H. Li, L. Shengkai, M. Yang, Y. Cao, L. Zhang, J. Wang, W.-Q. Cai, W.-Y. Liu, S.-L. Li, R. Shu, Y.-M. Huang, L. Deng, L. Li, Q. Zhang, N.-L. Liu, Y.-A. Chen, C.-Y. Lu, X.-B. Wang, and J.-W. Pan, "Entanglement-based secure quantum cryptography over 1,120 kilometres," *Nature*, vol. 582, pp. 1–5, 06 2020.

[41] S. K. Joshi, D. Aktas, S. Wengerowsky, M. Loncaric, S. P. Neumann, B. Liu, T. Scheidl, G. C. Lorenzo, Z. Samec, L. Kling, and et al., "A trusted node–free eight-user metropolitan quantum communication network," *Science Advances*, vol. 6, p. eaba0959, Sep 2020.

[42] "Quantum protocol zoo, https://wiki.veriqloud.fr/."

[43] C. Portmann and R. Renner, "Cryptographic security of quantum key distribution," *ArXiv*, vol. abs/1409.3525, 2014.

[44] E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, "Practical challenges in quantum key distribution," *npj Quant. Inf.*, vol. 2, p. 16025, 2016.

[45] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. R. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. S. Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, "Advances in quantum cryptography," *Adv. Opt. Photonics*, vol. 12, p. 1012, 2020.

[46] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Rev. Mod. Phys.*, vol. 81, pp. 1301–1350, Sep 2009.

[47] F. Laudenbach, C. Pacher, C.-H. F. Fung, A. Poppe, M. Peev, B. Schrenk, M. Hentschel, P. Walther, and H. Hübel, "Continuous-variable quantum key distribution with gaussian modulation-the theory of practical implementations," *Advanced Quantum Technologies*, vol. 1, p. 1800011, jun 2018.

[48] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theoretical Computer Science*, vol. 560, pp. 7–11, 2014.
Theoretical Aspects of Quantum Cryptography – celebrating 30 years of BB84.

[49] E. Bai, X.-q. Jiang, and Y. Wu, "Memory-saving and high-speed privacy amplification algorithm using lfsr-based hash function for key generation," *Electronics*, vol. 11, no. 3, 2022.

[50] D. Li, P. Huang, Y. Zhou, Y. Li, and G. Zeng, "Memory-saving implementation of high-speed privacy amplification algorithm for continuous-variable quantum key distribution," *IEEE Photonics Journal*, vol. 10, no. 5, pp. 1–12, 2018.

[51] A. K. Ekert, "Quantum cryptography based on bell's theorem," *Phys. Rev. Lett.*, vol. 67, pp. 661–663, Aug 1991.

[52] C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without bell's theorem," *Phys. Rev. Lett.*, vol. 68, pp. 557–559, Feb 1992.

[53] H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," *Physical Review Letters*, vol. 108, Mar 2012.

[54] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, "Overcoming the rate–distance limit of quantum key distribution without quantum repeaters," *Nature*, vol. 557, p. 400–403, May 2018.

[55] Y.-L. Tang, H.-L. Yin, Q. Zhao, H. Liu, X.-X. Sun, M.-Q. Huang, W.-J. Zhang, S.-J. Chen, L. Zhang, L.-X. You, Z. Wang, Y. Liu, C.-Y. Lu, X. Jiang, X. Ma, Q. Zhang, T.-Y. Chen, and J.-W. Pan, "Measurement-device-independent quantum key distribution over untrustful metropolitan network," *Phys. Rev. X*, vol. 6, p. 011024, Mar 2016.

[56] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, W.-J. Zhang, Z.-Y. Han, S.-Z. Ma, X.-L. Hu, Y.-H. Li, H. Liu, F. Zhou, H.-F. Jiang, T.-Y. Chen, H. Li, L.-X. You, Z. Wang, X.-B. Wang, Q. Zhang, and J.-W. Pan, "Twin-field quantum key distribution over 511 km optical fiber linking two distant metropolitans," 2021.

[57] B. Huttner, N. Imoto, N. Gisin, and T. Mor, "Quantum cryptography with coherent states," *Phys. Rev. A*, vol. 51, pp. 1863–1869, Mar 1995.

[58] N. Lütkenhaus and M. Jahma, "Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack," *New Journal of Physics*, vol. 4, pp. 44–44, jul 2002.

[59] H.-K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," *Physical Review Letters*, vol. 94, jun 2005.

[60] S. Fossier, E. Diamanti, T. Debuisschert, A. Villing, R. Tualle-Brouri, and P. Grangier, "Field test of a continuous-variable quantum key distribution prototype," *New Journal of Physics*, vol. 11, p. 045023, apr 2009.

[61] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, "Experimental demonstration of long-distance continuous-variable quantum key distribution," *Nature Photonics*, vol. 7, pp. 378–381, Oct 2013.

[62] H.-K. Lo and J. Preskill, "Security of quantum key distribution using weak coherent states with nonrandom phases," 2006.

[63] "Anssi: Should quantum key distribution be used for secure communications?."

[64] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, "Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels," *Phys. Rev. Lett.*, vol. 70, pp. 1895–1899, Mar 1993.

[65] M. Blum, "Coin flipping by telephone," in *Advances in Cryptology: A Report on CRYPTO 81*, pp. 11–15, 1981.

[66] H.-K. Lo and H. F. Chau, "Why quantum bit commitment and ideal quantum coin tossing are impossible," 1996.

[67] M. Bozzio, U. Chabaud, I. Kerenidis, and E. Diamanti, "Quantum weak coin flipping with a single photon," 2020.

[68] A. Pappa, A. Chailloux, E. Diamanti, and I. Kerenidis, "Practical quantum coin flipping," *Phys. Rev. A*, vol. 84, p. 052305, Nov 2011.

[69] D. Mayers, L. Salvail, and Y. Chiba-Kohno, "Unconditionally secure quantum coin tossing," 1999.

[70] M. O. Rabin, "How to exchange secrets with oblivious transfer," *IACR Cryptol. ePrint Arch.*, vol. 2005, p. 187, 2005.

[71] C. H. Bennett, G. Brassard, C. Crépeau, and M.-H. Skubiszewska, "Practical quantum oblivious transfer," in *Advances in Cryptology — CRYPTO '91* (J. Feigenbaum, ed.), (Berlin, Heidelberg), pp. 351–366, Springer Berlin Heidelberg, 1992.

[72] U. Maurer and J. Ribeiro, "New perspectives on weak oblivious transfer," in *2016 IEEE International Symposium on Information Theory (ISIT)*, pp. 790–794, July 2016.

[73] A. Kent, "Unconditionally secure bit commitment by transmitting measurement outcomes," *Physical Review Letters*, vol. 109, sep 2012.

[74] A. Broadbent, J. Fitzsimons, and E. Kashefi, "Universal blind quantum computation," *2009 50th Annual IEEE Symposium on Foundations of Computer Science*, Oct 2009.

[75] A. Broadbent, "Delegating private quantum computations," *Canadian Journal of Physics*, vol. 93, p. 941–946, Sep 2015.

[76] J. Fitzsimons, "Private quantum computation: An introduction to blind quantum computing and related protocols," *npj Quantum Information*, vol. 3, 11 2016.

[77] T. P. Spiller, K. Nemoto, S. L. Braunstein, W. J. Munro, P. van Loock, and G. J. Milburn, "Quantum computation by communication," *New Journal of Physics*, vol. 8, no. 2, p. 30, 2006.

[78] E. Kashefi, D. Leichtle, L. Music, and H. Ollivier, "Securing quantum computations in the nisq era," 2020.

[79] A. Cojocaru, L. Colisson, E. Kashefi, and P. Wallden, "Qfactory: Classically-instructed remote secret qubits preparation," *Advances in Cryptology – ASIACRYPT 2019*, p. 615–645, 2019.

[80] C. Badertscher, A. Cojocaru, L. Colisson, E. Kashefi, D. Leichtle, A. Mantri, and P. Wallden, "Security limitations of classical-client delegated quantum computing," *Lecture Notes in Computer Science*, p. 667–696, 2020.

[81] V. Dunjko, J. F. Fitzsimons, C. Portmann, and R. Renner, "Composable security of delegated quantum computation," in *Advances in Cryptology – ASIACRYPT 2014* (P. Sarkar and T. Iwata, eds.), (Berlin, Heidelberg), pp. 406–425, Springer Berlin Heidelberg, 2014.

[82] H. J. Briegel, D. E. Browne, W. Dür, R. Raussendorf, and M. Van den Nest, "Measurement-based quantum computation," *Nature Physics*, vol. 5, p. 19–26, Jan 2009.

[83] M. Navascués, E. Wolfe, D. Rosset, and A. Pozas-Kerstjens, "Genuine network multipartite entanglement," *Physical Review Letters*, vol. 125, Dec 2020.

[84] F. Grasselli, G. Murta, J. de Jong, F. Hahn, D. Bruß, H. Kampermann, and A. Pappa, "Robust anonymous conference key agreement enhanced by multipartite entanglement," 2021.

[85] A. Pappa, A. Chailloux, S. Wehner, E. Diamanti, and I. Kerenidis, "Multipartite entanglement verification resistant against dishonest parties," *Physical Review Letters*, vol. 108, 12 2011.

[86] W. McCutcheon, A. Pappa, B. Bell, A. McMillan, A. Chailloux, T. Lawson, M. Mafu, D. Markham, E. Diamanti, I. Kerenidis, J. Rarity, and M. Tame, "Experimental verification of multipartite entanglement in quantum networks," *Nature Communications*, vol. 7, p. 13251, 11 2016.

[87] G. Murta, F. Grasselli, H. Kampermann, and D. Bruß, "Quantum conference key agreement: A review," *Advanced Quantum Technologies*, vol. 3, p. 2000025, Sep 2020.

[88] F. Hahn, J. de Jong, and A. Pappa, "Anonymous quantum conference key agreement," *PRX Quantum*, vol. 1, Dec 2020.

[89] F. Grasselli, H. Kampermann, and D. Bruß, "Finite-key effects in multipartite quantum key distribution protocols," *New Journal of Physics*, vol. 20, p. 113014, Nov 2018.

[90] M. Proietti, J. Ho, F. Grasselli, P. Barrow, M. Malik, and A. Fedrizzi, "Experimental quantum conference key agreement," *Science Advances*, vol. 7, p. eabe0395, Jun 2021.

[91] M. Christandl and S. Wehner, "Quantum anonymous transmissions," in *International Conference on the Theory and Application of Cryptology and Information Security*, pp. 217–235, Springer, 2005.

[92] G. Brassard, A. Broadbent, J. Fitzsimons, S. Gambs, and A. Tapp, "Anonymous quantum communication," in *International Conference on the Theory and Application of Cryptology and Information Security*, pp. 460–473, Springer, 2007.

[93] A. Unnikrishnan, I. MacFarlane, R. Yi, E. Diamanti, D. Markham, and I. Kerenidis, "Anonymity for practical quantum networks," *Physical Review Letters*, vol. 122, 11 2018.

[94] L. Lamport, R. Shostak, and M. Pease, "The byzantine generals problem," *ACM Trans. Program. Lang. Syst.*, vol. 4, p. 382–401, jul 1982.

[95] M. Ben-Or and A. Hassidim, "Fast quantum byzantine agreement," in *Proceedings of the Thirty-Seventh Annual ACM Symposium on Theory of Computing*, STOC '05, (New York, NY, USA), p. 481–485, Association for Computing Machinery, 2005.

[96] M. Fitzi, N. Gisin, and U. Maurer, "Quantum solution to the byzantine agreement problem," *Physical Review Letters*, vol. 87, nov 2001.

[97] X. Sun, P. Kulicki, and M. Sopek, "Multi-party quantum byzantine agreement without entanglement," *Entropy*, vol. 22, p. 1152, oct 2020.

[98] Y. Feng, R. Shi, J. Zhou, Q. Liao, and Y. Guo, "Quantum byzantine agreement with tripartite entangled states," *International Journal of Theoretical Physics*, vol. 58, 05 2019.

[99] S. Gaertner, M. Bourennane, C. Kurtsiefer, A. Cabello, and H. Weinfurter, "Experimental demonstration of a quantum protocol for byzantine agreement and liar detection," *Physical Review Letters*, vol. 100, feb 2008.

[100] M. Ganz, "Quantum leader election," 2009.

[101] F. Centrone, E. Diamanti, and I. Kerenidis, "Practical quantum electronic voting," *arXiv preprint arXiv:2107.14719*, 2021.

[102] M. Clementi, A. Pappa, A. Eckstein, I. A. Walmsley, E. Kashefi, and S. Barz, "Classical multiparty computation using quantum resources," *Physical Review A*, vol. 96, dec 2017.

[103] E. Kashefi and A. Pappa, "Multiparty Delegated Quantum Computing," *Cryptography*, vol. 1, p. 12, July 2017.

[104] M. Bozzio, A. Orieux, L. Trigo Vidarte, I. Zaquine, I. Kerenidis, and E. Diamanti, "Experimental investigation of practical unforgeable quantum money," *npj Quantum Information*, vol. 4, Jan 2018.

[105] M. Bozzio, E. Diamanti, and F. Grosshans, "Semi-device-independent quantum money with coherent states," *Physical Review A*, vol. 99, p. 022336, Feb. 2019.

[106] R. Jozsa, D. S. Abrams, J. P. Dowling, and C. P. Williams, "Quantum clock synchronization based on shared prior entanglement," *Physical Review Letters*, vol. 85, no. 9, p. 2010, 2000.

[107] M. Krčo and P. Paul, "Quantum clock synchronization: Multiparty protocol," *Physical Review A*, vol. 66, no. 2, p. 024305, 2002.

[108] J. Preskill, "Quantum clock synchronization and quantum error correction," *arXiv preprint quant-ph/0010098*, 2000.

[109] V. Giovannetti, S. Lloyd, and L. Maccone, "Quantum-enhanced positioning and clock synchronization," *Nature*, vol. 412, no. 6845, pp. 417–419, 2001.

[110] U. Maurer and R. Renner, "Abstract cryptography," *In Innovations In Computer Science*, 2011.

[111] U. Maurer and R. Renner, "From indifferentiability to constructive cryptography (and back)," in *Theory of Cryptography*, (Berlin, Heidelberg), pp. 3–24, Springer Berlin Heidelberg, 2016.

[112] U. Maurer, "Constructive cryptography - a new paradigm for security definitions and proofs," *IN Theory of Security and Applications*, pp. 33–56, 2011.

[113] R. Canetti, "Universally composable security: A new paradigm for cryptographic protocols." Cryptology ePrint Archive, Report 2000/067, 2000.

[114] G. Demay and U. Maurer, "Unfair coin tossing," *2013 IEEE International Symposium on Information Theory*, pp. 1556–1560, 2013.

[115] A. Gheorghiu and T. Vidick, "Computationally-secure and composable remote state preparation," *ArXiv*, vol. abs/1904.06320, 2019.

[116] M. Houshmand, M. Houshmand, S.-H. Tan, and J. Fitzsimons, "Composable secure multi-client delegated quantum computation," *ArXiv*, vol. abs/1811.11929, 2018.

[117] V. Vilasini, C. Portmann, and L. del Rio, "Composable security in relativistic quantum cryptography," *New Journal of Physics*, vol. 21, p. 043057, apr 2019.

[118] D. Jost, U. Maurer, and M. Mularczyk, "A unified and composable take on ratcheting." Cryptology ePrint Archive, Report 2019/694, 2019.

[119] W. Huang, Q.-Y. Wen, B. Liu, Q. Su, S.-J. Qin, and F. Gao, "Quantum anonymous ranking," *Phys. Rev. A*, vol. 89, p. 032325, Mar 2014.

[120] M. Hillery, V. Bužek, and A. Berthiaume, "Quantum secret sharing," *Physical Review A*, vol. 59, p. 1829–1834, Mar 1999.

[121] E. D'Hondt and P. Panangaden, "Leader election and distributed consensus with quantum resources," 2004.

[122] A. Unnikrishnan and D. Markham, "Verification of graph states in an untrusted network," *Physical Review A*, 07 2020.

[123] S. K. Singh, S. P. Pal, S. Kumar, and R. Srikanth, "A combinatorial approach for studying LOCC transformations of multipartite states," 2004.

[124] A. Broadbent and A. Tapp, "Information-theoretic security without an honest majority," in *Advances in Cryptology – ASIACRYPT 2007* (K. Kurosawa, ed.), (Berlin, Heidelberg), pp. 410–426, Springer Berlin Heidelberg, 2007.

[125] R. Canetti, Y. Lindell, R. Ostrovsky, and A. Sahai, "Universally composable two-party and multi-party secure computation," *Conference Proceedings of the Annual ACM Symposium on Theory of Computing*, 08 2003.

[126] J. L. Park, "The concept of transition in quantum mechanics," *Foundations of Physics*, vol. 1, no. 1, pp. 23–33, 1970.

[127] M. Takeoka, S. Guha, and M. M. Wilde, "Fundamental rate-loss tradeoff for optical quantum key distribution," *Nature Communications*, vol. 5, p. 5235, 2014.

[128] M. Takeoka, S. Guha, and M. M. Wilde, "The squashed entanglement of a quantum channel," *Information Theory, IEEE Transactions on*, vol. 60, no. 8, pp. 4987–4998, 2014.

[129] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, "Fundamental limits of repeaterless quantum communications," *Nature Communications*, vol. 8, pp. 15043 EP –, 04 2017.

[130] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, "Quantum repeaters: The role of imperfect local operations in quantum communication," *Physical Review Letters*, vol. 81, no. 26, p. 5932, 1998.

[131] N. Sangouard, C. Simon, H. De Riedmatten, and N. Gisin, "Quantum repeaters based on atomic ensembles and linear optics," *Reviews of Modern Physics*, vol. 83, no. 1, p. 33, 2011.

[132] W. J. Munro, K. Azuma, K. Tamaki, and K. Nemoto, "Inside quantum repeaters," *Selected Topics in Quantum Electronics, IEEE Journal of*, vol. 21, no. 3, pp. 1–13, 2015.

[133] H. J. Kimble, "The quantum internet," *Nature*, vol. 453, no. 7198, p. 1023, 2008.

[134] W. Dür, H.-J. Briegel, J. Cirac, and P. Zoller, "Quantum repeaters based on entanglement purification," *Physical Review A*, vol. 59, no. 1, p. 169, 1999.

[135] L.-M. Duan, M. Lukin, J. I. Cirac, and P. Zoller, "Long-distance quantum communication with atomic ensembles and linear optics," *Nature*, vol. 414, no. 6862, pp. 413–418, 2001.

[136] C. Simon, H. De Riedmatten, M. Afzelius, N. Sangouard, H. Zbinden, and N. Gisin, "Quantum repeaters with photon pair sources and multimode memories," *Physical Review Letters*, vol. 98, no. 19, p. 190503, 2007.

[137] N. Sangouard, C. Simon, B. Zhao, Y.-A. Chen, H. De Riedmatten, J.-W. Pan, and N. Gisin, "Robust and efficient quantum repeaters with atomic ensembles and linear optics," *Physical Review A*, vol. 77, no. 6, p. 062301, 2008.

[138] L. Jiang, J. M. Taylor, K. Nemoto, W. J. Munro, R. Van Meter, and M. D. Lukin, "Quantum repeater with encoding," *Physical Review A*, vol. 79, no. 3, p. 032325, 2009.

[139] N. K. Bernardes and P. van Loock, "Hybrid quantum repeater with encoding," *Physical Review A*, vol. 86, no. 5, p. 052301, 2012.

[140] K. Azuma, K. Tamaki, and H.-K. Lo, "All-photonic quantum repeaters," *Nature Communications*, vol. 6, 2015.

[141] D. Luong, L. Jiang, J. Kim, and N. Lütkenhaus, "Overcoming lossy channel bounds using a single quantum repeater node," *Applied Physics B*, vol. 122, no. 4, pp. 1–10, 2016.

[142] P. C. Humphreys, N. Kalb, J. P. Morits, R. N. Schouten, R. F. Vermeulen, D. J. Twitchen, M. Markham, and R. Hanson, "Deterministic delivery of remote entanglement on a quantum network," *Nature*, vol. 558, no. 7709, p. 268, 2018.

[143] T. H. Taminiau, J. Cramer, T. van der Sar, V. V. Dobrovitski, and R. Hanson, "Universal control and error correction in multi-qubit spin registers in diamond," *Nature Nanotechnology*, vol. 9, no. 3, pp. 171–176, 2014.

[144] S. B. van Dam, P. C. Humphreys, F. Rozpędek, S. Wehner, and R. Hanson, "Multiplexed entanglement generation over quantum networks using multi-qubit nodes," *Quantum Science and Technology*, vol. 2, no. 3, p. 034002, 2017.

[145] M. Blok, N. Kalb, A. Reiserer, T. Taminiau, and R. Hanson, "Towards quantum networks of single spins: analysis of a quantum memory with an optical interface in diamond," *Faraday Discussions*, vol. 184, pp. 173–182, 2015.

[146] J. Cramer, N. Kalb, M. A. Rol, B. Hensen, M. S. Blok, M. Markham, D. J. Twitchen, R. Hanson, and T. H. Taminiau, "Repeated quantum error correction on a continuously encoded qubit by real-time feedback," *Nature Communications*, vol. 7, 2016.

[147] A. Reiserer, N. Kalb, M. S. Blok, K. J. van Bemmelen, T. H. Taminiau, R. Hanson, D. J. Twitchen, and M. Markham, "Robust quantum-network memory using decoherence-protected subspaces of nuclear spins," *Physical Review X*, vol. 6, no. 2, p. 021040, 2016.

[148] W. Gao, A. Imamoglu, H. Bernien, and R. Hanson, "Coherent manipulation, measurement and entanglement of individual solid-state spins using optical fields," *Nature Photonics*, vol. 9, no. 6, pp. 363–373, 2015.

[149] S. Bogdanovic, S. B. van Dam, C. Bonato, L. C. Coenen, A. Zwerver, B. Hensen, M. S. Liddy, T. Fink, A. Reiserer, M. Loncar, and R. Hanson, "Design and low-temperature characterization of a tunable microcavity for diamond-based quantum networks," *Applied Physics Letters*, vol. 110, no. 17, p. 171103, 2017.

[150] C. Cabrillo, J. I. Cirac, P. Garcia-Fernandez, and P. Zoller, "Creation of entangled states of distant atoms by interference," *Physical Review A*, vol. 59, no. 2, p. 1025, 1999.

[151] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *International Conference on Computer System and Signal Processing, IEEE, 1984*, pp. 175–179, 1984.

[152] D. Bruß, "Optimal eavesdropping in quantum cryptography with six states," *Physical Review Letters*, vol. 81, no. 14, p. 3018, 1998.

[153] H. Bechmann-Pasquinucci and N. Gisin, "Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography," *Physical Review A*, vol. 59, no. 6, p. 4238, 1999.

[154] S. Pirandola, "Capacities of repeater-assisted quantum communications," *arXiv preprint arXiv:1601.00966*, 2016.

[155] S. D. Barrett and P. Kok, "Efficient high-fidelity quantum computation using matter qubits and linear optics," *Physical Review A*, vol. 71, no. 6, p. 060310, 2005.

[156] B. Hensen, H. Bernien, A. Dréau, A. Reiserer, N. Kalb, M. Blok, J. Ruitenberg, R. Vermeulen, R. Schouten, C. Abellán, *et al.*, "Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres," *Nature*, vol. 526, no. 7575, pp. 682–686, 2015.

[157] B. Hensen, N. Kalb, M. Blok, A. Dréau, A. Reiserer, R. Vermeulen, R. Schouten, M. Markham, D. Twitchen, K. Goodenough, *et al.*, "Loophole-free bell test using electron spins in diamond: second experiment and additional analysis," *Scientific Reports*, vol. 6, 2016.

[158] H. Bernien, B. Hensen, W. Pfaff, G. Koolstra, M. Blok, L. Robledo, T. Taminiau, M. Markham, D. Twitchen, L. Childress, *et al.*, "Heralded entanglement between solid-state qubits separated by three metres," *Nature*, vol. 497, no. 7447, p. 86, 2013.

[159] P. Maunz, D. Moehring, S. Olmschenk, K. Younge, D. Matsukevich, and C. Monroe, "Quantum interference of photon pairs from two remote trapped atomic ions," *Nature Physics*, vol. 3, no. 8, p. 538, 2007.

[160] R. Stockill, M. Stanley, L. Huthmacher, E. Clarke, M. Hugues, A. Miller, C. Matthiesen, C. Le Gall, and M. Atatüre, "Phase-tuned entangled state generation between distant spin qubits," *Physical Review Letters*, vol. 119, no. 1, p. 010503, 2017.

[161] A. Delteil, Z. Sun, W.-b. Gao, E. Togan, S. Faelt, and A. Imamoğlu, "Generation of heralded entanglement between distant hole spins," *Nature Physics*, vol. 12, no. 3, p. 218, 2016.

[162] C. W. Chou, H. de Riedmatten, D. Felinto, S. V. Polyakov, S. J. van Enk, and H. J. Kimble, "Measurement-induced entanglement for excitation stored in remote atomic ensembles," *Nature*, vol. 438, pp. 828 EP –, Dec 2005.

[163] K. Tamaki, H.-K. Lo, W. Wang, and M. Lucamarini, "Information theoretic security of quantum key distribution overcoming the repeaterless secret key capacity bound," *arXiv preprint arXiv:1805.05511*, 2018.

[164] X. Ma, P. Zeng, and H. Zhou, "Phase-matching quantum key distribution," *Physical Review X*, vol. 8, no. 3, p. 031043, 2018.

[165] J. S. Ivan, K. K. Sabapathy, and R. Simon, "Operator-sum representation for bosonic gaussian channels," *Physical Review A*, vol. 84, no. 4, p. 042311, 2011.

[166] M. W. Doherty, N. B. Manson, P. Delaney, F. Jelezko, J. Wrachtrup, and L. C. L. Hollenberg, "The nitrogen-vacancy colour centre in diamond," *Physics Reports*, vol. 528, no. 1, pp. 1–45, 2013.

[167] N. Kalb, P. Humphreys, J. Slim, and R. Hanson, "Dephasing mechanisms of diamond-based nuclear-spin memories for quantum networks," *Physical Review A*, vol. 97, no. 6, p. 062330, 2018.

[168] W. Pfaff, B. Hensen, H. Bernien, S. B. van Dam, M. S. Blok, T. H. Taminiau, M. J. Tiggelman, R. N. Schouten, M. Markham, D. J. Twitchen, *et al.*, "Unconditional quantum teleportation between distant solid-state quantum bits," *Science*, vol. 345, no. 6196, pp. 532–535, 2014.

[169] E. M. Purcell, H. C. Torrey, and R. V. Pound, "Resonance Absorption by Nuclear Magnetic Moments in a Solid," *Physical Review*, vol. 69, no. 1-2, pp. 37–38, 1946.

[170] D. Englund, B. Shields, K. Rivoire, F. Hatami, J. Vučković, H. Park, and M. D. Lukin, "Deterministic coupling of a single nitrogen vacancy center to a photonic crystal cavity," *Nano Letters*, vol. 10, no. 10, pp. 3922–3926, 2010.

[171] J. Wolters, A. W. Schell, G. Kewes, N. Nüsse, M. Schoengen, H. Döscher, T. Hannappel, B. Löchel, M. Barth, and O. Benson, "Enhancement of the zero phonon line emission from a single nitrogen vacancy center in a nanodiamond via coupling to a photonic crystal cavity," *Applied Physics Letters*, vol. 97, no. 14, pp. 2008–2011, 2010.

[172] T. Van Der Sar, J. Hagemeier, W. Pfaff, E. C. Heeres, S. M. Thon, H. Kim, P. M. Petroff, T. H. Oosterkamp, D. Bouwmeester, and R. Hanson, "Deterministic nanoassembly of a coupled quantum emitter-photonic crystal cavity system," *Applied Physics Letters*, vol. 98, no. 19, pp. 1–4, 2011.

[173] A. Faraon, C. Santori, Z. Huang, V. M. Acosta, and R. G. Beausoleil, "Coupling of nitrogen-vacancy centers to photonic crystal cavities in monocrystalline diamond," *Physical Review Letters*, vol. 109, no. 3, pp. 2–6, 2012.

[174] B. J. Hausmann, B. J. Shields, Q. Quan, Y. Chu, N. P. De Leon, R. Evans, M. J. Burek, A. S. Zibrov, M. Markham, D. J. Twitchen, H. Park, M. D. Lukin, and M. Loncar, "Coupling of NV centers to photonic crystal nanobeams in diamond," *Nano Letters*, vol. 13, no. 12, pp. 5791–5796, 2013.

[175] J. C. Lee, D. O. Bracher, S. Cui, K. Ohno, C. A. McLellan, X. Zhang, P. Andrich, B. Alemán, K. J. Russell, A. P. Magyar, I. Aharonovich, A. Bleszynski Jayich, D. Awschalom, and E. L. Hu, "Deterministic coupling of delta-doped nitrogen vacancy centers to a nanobeam photonic crystal cavity," *Applied Physics Letters*, vol. 105, no. 26, 2014.

[176] L. Li, T. Schröder, E. H. Chen, M. Walsh, I. Bayn, J. Goldstein, O. Gaathon, M. E. Trusheim, M. Lu, J. Mower, M. Cotlet, M. L. Markham, D. J. Twitchen, and D. Englund, "Coherent spin control of a nanocavity-enhanced qubit in diamond," *Nature Communications*, vol. 6, 2015.

[177] J. Riedrich-Möller, S. Pezzagna, J. Meijer, C. Pauly, F. Mücklich, M. Markham, A. M. Edmonds, and C. Becher, "Nanoimplantation and Purcell enhancement of single nitrogen-vacancy centers in photonic crystal cavities in diamond," *Applied Physics Letters*, vol. 106, no. 22, pp. 1–5, 2015.

[178] A. Faraon, P. E. Barclay, C. Santori, K. M. C. Fu, and R. G. Beausoleil, "Resonant enhancement of the zero-phonon emission from a colour centre in a diamond cavity," *Nature Photonics*, vol. 5, no. 5, pp. 301–305, 2011.

[179] P. E. Barclay, K. M. C. Fu, C. Santori, A. Faraon, and R. G. Beausoleil, "Hybrid nanocavity resonant enhancement of color center emission in diamond," *Physical Review X*, vol. 1, no. 1, pp. 1–7, 2011.

[180] M. Gould, E. R. Schmidgall, S. Dadgostar, F. Hatami, and K. M. C. Fu, "Efficient Extraction of Zero-Phonon-Line Photons from Single Nitrogen-Vacancy Centers in an Integrated GaP-on-Diamond Platform," *Physical Review Applied*, vol. 6, no. 1, pp. 2–7, 2016.

[181] H. Kaupp, C. Deutsch, H. C. Chang, J. Reichel, T. W. Hänsch, and D. Hunger, "Scaling laws of the cavity enhancement for nitrogen-vacancy centers in diamond," *Physical Review A*, vol. 88, no. 5, pp. 1–8, 2013.

[182] S. Johnson, P. R. Dolan, T. Grange, A. A. Trichet, G. Hornecker, Y. C. Chen, L. Weng, G. M. Hughes, A. A. Watt, A. Auffèves, and J. M. Smith, "Tunable cavity coupling of the zero phonon line of a nitrogen-vacancy defect in diamond," *New Journal of Physics*, vol. 17, no. 12, 2015.

[183] D. Riedel, I. Söllner, B. J. Shields, S. Starosielec, P. Appel, E. Neu, P. Maletinsky, and R. J. Warburton, "Deterministic enhancement of coherent photon generation from a nitrogen-vacancy center in ultrapure diamond," *Physical Review X*, vol. 7, no. 3, p. 031040, 2017.

[184] D. Hunger, T. Steinmetz, Colombe, Y., C. Deutsch, T. W. Hänsch, and J. Reichel, "A fiber Fabry-Perot cavity with high finesse," *New Journal of Physics*, vol. 12, 2010.

[185] E. Janitz, M. Ruf, M. Dimock, A. Bourassa, J. Sankey, and L. Childress, "Fabry-Perot microcavity for diamond-based photonics," *Physical Review A*, vol. 92, no. 4, pp. 1–11, 2015.

[186] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Reviews of Modern Physics*, vol. 81, no. 3, p. 1301, 2009.

[187] S. Watanabe, R. Matsumoto, T. Uyematsu, and Y. Kawano, "Key rate of quantum key distribution with hashed two-way classical communication," *Physical Review A*, vol. 76, no. 3, p. 032312, 2007.

[188] H.-K. Lo, H. F. Chau, and M. Ardehali, "Efficient quantum key distribution scheme and a proof of its unconditional security," *Journal of Cryptology*, vol. 18, no. 2, pp. 133–165, 2005.

[189] A. Khalique and B. C. Sanders, "Practical long-distance quantum key distribution through concatenated entanglement swapping with parametric down-conversion sources," *JOSA B*, vol. 32, no. 11, pp. 2382–2390, 2015.

[190] H. Krovi, S. Guha, Z. Dutton, J. A. Slater, C. Simon, and W. Tittel, "Practical quantum repeaters with parametric down-conversion sources," *Applied Physics B*, vol. 122, no. 3, pp. 1–8, 2016.

[191] M. Pant, H. Krovi, D. Englund, and S. Guha, "Rate-distance tradeoff and resource costs for all-optical quantum repeaters," *Physical Review A*, vol. 95, no. 1, p. 012304, 2017.

[192] S. Guha, H. Krovi, C. A. Fuchs, Z. Dutton, J. A. Slater, C. Simon, and W. Tittel, "Rate-loss analysis of an efficient quantum repeater architecture," *Physical Review A*, vol. 92, no. 2, p. 022357, 2015.

[193] K. Goodenough, D. Elkouss, and S. Wehner, "Assessing the performance of quantum repeaters for all phase-insensitive gaussian bosonic channels," *New Journal of Physics*, vol. 18, no. 6, p. 063005, 2016.

[194] E. Kaur and M. M. Wilde, "Upper bounds on secret-key agreement over lossy thermal bosonic channels," *Physical Review A*, vol. 96, no. 6, p. 062318, 2017.

[195] K. Sharma, M. M. Wilde, S. Adhikari, and M. Takeoka, "Bounding the energy-constrained quantum and private capacities of phase-insensitive bosonic gaussian channels," *New Journal of Physics*, vol. 20, no. 6, p. 063025, 2018.

[196] N. Davis, M. E. Shirokov, and M. M. Wilde, "Energy-constrained two-way assisted private and quantum capacities of quantum channels," *Physical Review A*, vol. 97, no. 6, p. 062310, 2018.

[197] C. Ottaviani, R. Laurenza, T. P. Cope, G. Spedalieri, S. L. Braunstein, and S. Pirandola, "Secret key capacity of the thermal-loss channel: Improving the lower bound," in *Quantum Information Science and Technology II*, vol. 9996, p. 999609, International Society for Optics and Photonics, 2016.

[198] M. Fox, *Quantum optics: an introduction*, vol. 15.
Oxford University Press, 2006.

[199] R. Paschotta, "Article on 'fibers' in *Encyclopedia of Laser Physics and Technology*."

[200] S. Zaske, A. Lenhard, C. A. Keßler, J. Kettler, C. Hepp, C. Arend, R. Albrecht, W.-M. Schulz, M. Jetter, P. Michler, *et al.*, "Visible-to-telecom quantum frequency conversion of light from a single quantum emitter," *Physical Review Letters*, vol. 109, no. 14, p. 147404, 2012.

[201] G. M. et al., "2022 roadmap on integrated quantum photonics," *J. Phys: Photonics*, vol. 4, p. 012501, 2022.

[202] "Netsquid website, https://netsquid.org/."

[203] R. Yehia, "Github repository for the netsquid simulation modules, https://github.com/rajayehia/quantumcity."

[204] M. Bozzio, M. Vyvlecka, M. Cosacchi, C. Nawrath, T. Seidelmann, J. C. Loredo, S. L. Portalupi, V. M. Axt, P. Michler, and P. Walther, "Enhancing quantum cryptography with quantum dot single-photon sources," 2022.

[205] D. Bouwmeester, J.-W. Pan, M. Daniell, H. Weinfurter, and A. Zeilinger, "Observation of three-photon greenberger-horne-zeilinger entanglement," *Physical Review Letters*, vol. 82, no. 7, p. 1345, 1999.

[206] J. Calsamiglia and N. Lütkenhaus, "Maximum efficiency of a linear-optical bell-state analyzer," *Applied Physics B*, vol. 72, no. 1, pp. 67–71, 2001.

[207] R.-B. Jin, R. Shimizu, I. Morohashi, K. Wakui, M. Takeoka, S. Izumi, T. Sakamoto, M. Fujiwara, T. Yamashita, S. Miki, *et al.*, "Efficient generation of twin photons at telecom wavelengths with 2.5 ghz repetition-rate-tunable comb laser," *Scientific reports*, vol. 4, no. 1, pp. 1–6, 2014.

[208] M. Leifgen, T. Schröder, F. Gädeke, R. Riemann, V. Métillon, E. Neu, C. Hepp, C. Arend, C. Becher, K. Lauritsen, and O. Benson, "Evaluation of nitrogen- and silicon-vacancy defect centres as single photon sources in quantum key distribution," *New Journal of Physics*, vol. 16, p. 023021, feb 2014.

[209] F. Rozpedek, R. Yehia, K. Goodenough, M. Ruf, P. C. Humphreys, R. Hanson, S. Wehner, and D. Elkouss, "Near-term quantum-repeater experiments with nitrogen-vacancy centers: Overcoming the limitations of direct transmission," *Phys. Rev. A*, vol. 99, p. 052330, May 2019.

[210] H.-K. Lo and J. Preskill, "Security of quantum key distribution using weak coherent states with nonrandom phases," *Quantum Info. Comput.*, vol. 7, p. 431–458, July 2007.

[211] E. Diamanti and A. Leverrier, "Distributing secret keys with quantum continuous variables: Principle, security and implementations," *Entropy*, vol. 17, pp. 6072–6092, 2015.

[212] A. Mantri, C. A. Pérez-Delgado, and J. F. Fitzsimons, "Optimal blind quantum computation," *Physical Review Letters*, vol. 111, Dec 2013.

[213] D. Istrati, Y. Pilnyak, J. C. Loredo, C. Antón, N. Somaschi, P. Hilaire, H. Ollivier, M. Esmann, L. Cohen, L. Vidro, C. Millet, A. Lemaître, I. Sagnes, A. Harouri, L. Lanco, P. Senellart, and H. S. Eisenberg, "Sequential generation of linear cluster states from a single photon emitter," *Nature Communications*, vol. 11, p. 5501, 2020.

[214] D. Dequal, L. Trigo Vidarte, V. Roman Rodriguez, G. Vallone, P. Villoresi, A. Leverrier, and E. Diamanti, "Feasibility of satellite-to-ground continuous-variable quantum key distribution," *npj Quantum Information*, vol. 7, Jan 2021.

[215] F. X. Kneizys, E. P. Shettle, L. W. Abreu, J. H. Chetwynd, and G. P. Anderson, *Users Guide to LOWTRAN 7*.
Air Force Geophysics Laboratory, 1988.

[216] F. X. Kneizys, "Atmospheric transmittance and radiance: The lowtran code," in *Optical Properties of the Atmosphere*, vol. 142, pp. 6–8, International Society for Optics and Photonics, 1978.

[217] D. Y. Vasylyev, A. A. Semenov, and W. Vogel, "Toward global quantum communication: Beam wandering preserves nonclassicality," *Phys. Rev. Lett.*, vol. 108, p. 220501, Jun 2012.

[218] D. Vasylyev, W. Vogel, and F. Moll, "Satellite-mediated quantum atmospheric links," *Physical Review A*, vol. 99, May 2019.

[219] "https://www.n2yo.com/."

[220] "orekit library, https://www.orekit.org/."

[221] B. Klein and J. Degnan, "Optical antenna gain 1: Transmitting antennas," *Applied optics*, vol. 13, pp. 2134–41, 09 1974.

[222] V. M. Acosta, D. Dequal, M. Schiavon, A. Montmerle-Bonnefois, C. B. Lim, J.-M. Conan, and E. Diamanti, "Analysis of satellite-to-ground quantum key distribution with adaptive optics," 2021.

[223] 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*, vol. 7, jan 2021.

[224] A. Seri, D. Lago-Rivera, G. Corrielli, A. Lenhard, R. Osellame, M. Mazzera, and H. de Riedmatten, "Quantum storage of frequency-multiplexed heralded single photons," in *2019 Conference on Lasers and Electro-Optics Europe and European Quantum Electronics Conference*, Optica Publishing Group, 2019.

[225] D. Lago-Rivera, S. Grandi, J. V. Rakonjac, A. Seri, and H. de Riedmatten, "Telecom-heralded entanglement between multimode solid-state quantum memories," *Nature*, vol. 594, p. 030501, Jun 2021.

[226] I. L. Chuang, D. W. Leung, and Y. Yamamoto, "Bosonic quantum codes for amplitude damping," *Physical Review A*, vol. 56, no. 2, p. 1114, 1997.

[227] O. Gittsovich, N. J. Beaudry, V. Narasimhachar, R. R. Alvarez, T. Moroder, and N. Lütkenhaus, "Squashing model for detectors and applications to quantum-key-distribution protocols," *Physical Review A*, vol. 89, no. 1, p. 012325, 2014.

[228] S. R. Jammalamadaka and A. Sengupta, *Topics in circular statistics*, vol. 5. World Scientific, 2001.

[229] G. Murta, F. Rozpędek, J. Ribeiro, D. Elkouss, and S. Wehner, "Key rates for quantum key distribution protocols with asymmetric noise," *Phys. Rev. A*, vol. 101, p. 062321, Jun 2020.

[230] R. Renner, "Eth zurich phd thesis," *arXiv preprint quant-ph/0512258*, 2005.

[231] H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," *Physical Review Letters*, vol. 108, no. 13, p. 130503, 2012.

[232] M. Lucamarini, Z. Yuan, J. F. Dynes, and A. J. Shields, "Overcoming the rate–distance limit of quantum key distribution without quantum repeaters," *Nature*, vol. 557, p. 400–403, May 2018.