TU DELFT

MSC. APPLIED PHYSICS

A spectrally-multiplexed Bell-state measurements

Towards multiplexed quantum repeaters

Author
Oriol PIETX I CASAS

Supervisors
Gustavo CASTRO DO AMARAL
Wolfgang TITTEL

September 28, 2020

Welcome to Oriol Pietx i Casas's Master thesis project main report.

This project was carried out during the 2019-2020 academic year in Wolfgang Tittel's group within QuTech, TU Delft, in the Netherlands. It is the final project for the MSc Applied Physics (Quantum devices and quantum technologies).

We hope the reader enjoys this work.

Contents

Before this thesis kicks-off we wanted to provide to the reader who is not familiar with physics, a little overview of what a quantum repeater is using an analogy of childhood...

A significant part of us, when an innocent child, has played the game of the telephone. For those who did not have the opportunity, you would line up with your friends with the goal to bring a message from one end to the other by whispering into the next person in line. Obviously there is no fun in just shouting the message, hoping the other end will get it, as everyone else in recess would come to discover your message. Running to the other end is also forbidden as no one has fun like that and it is exhausting...

As an example, imagine a school class. We have Alice who likes Bianca, but she is too shy to go and tell her. Every once in a while, she finds the courage to stand up and run across the park to find her. However, as she goes and gets closer and closer, her confidence drops and she starts getting nervous, to the point that when she is standing in front of Bianca she is confused, does not find the right words, and only manages to mumble nonsense. Bianca is left completely confused- *What does Alice want?* One day Alice has a wonderful idea: she convinces all her best friends to play the telephone game. She will stand on one end and, mischievously, they will place Bianca at the other end. She has found the game to be the perfect means to let Bianca know she is in love with her without actually having to tell her in person. Also because she is actually just telling her secret to a good friend of hers, she can say it loud and clear. Her best friends would never spill out the message so someone else could hear it, it is forbidden by the best-friends-forever code.

Alice, however, has played the game many times before and knows that usually only parts of the initial message will get to Bianca even if everyone is trying their best; after all they are kids during recess. Who can keep them quiet and forming a line? We can only hope that the chain they are forming is stable enough and that they are ready to pass on the message when it is their turn so that Bianca gets to know Alice's feelings for her. Also, it is obvious that fewer people participating in the game makes the outcome more reliable and easy to obtain.

The day has arrived. Alice is positive and confident that her message will be received, she has found two good solution to compensate for the little linklets not paying attention: (i) the linklets will send a message from the center to the outer parts of the chain by squeezing their hands, effectively notifying Alice and Bianca that the chain is ready to forward the message; (ii) since Alice has many friends, she can arrange them in multiple chains, one next to the other, all converging on her and Bianca's end. That way, she avoids relying only on one single set of friends having to be ready and cooperate simultaneously. Her secret will, hopefully, make it through at least one of the chains in one piece, not giving Bianca any room for misinterpretation.

It is a success! Now the new couple in school, Bianca and Alice, can sit next to each other during the classes in an awkward silence. Isn't primary school the best..?

The reader to whom the words *"multiplexed quantum repeater architecture"* do not mean anything might be surprised by this brief introduction to the work. I will try my best, in the following text, to relate the lovely story of Alice and Bianca to the practical technology studied in this thesis. To the more experienced reader, let this be a quite inaccurate refresher or just an anecdote.

Abstract

In this master's thesis we report on the characterization of spectral-multiplexed Bell-state measurement, a fundamental building block of spectral-multiplexed quantum repeater architecture. To test our hypothesis, we show an experimental setup that resembles an MDI-QKD setup, but multiplexed in frequency. The result is an increased secret key rate thanks to the individual contributions of each spectral mode. We also report characterization of all relevant degrees of freedom that affect Bell-state measurement efficiency, such as spectral-demultiplexing, Hong-Ou-Mandel interference and qubit generation. To finalize, we discuss on possible improvements and lay down the steps to follow to achieve spectrally-multiplexed quantum teleportation.

In this first section we present and motivate the entire work from a "big picture" point of view: the idea of quantum repeater is introduced and some insights of the frequency-multiplexed quantum repeater architecture and its protocol to distribute entanglement are given...

1 Introduction

Here in Delft, there is a project to launch a small-scale quantum network shared by a few universities. Though it may seem a bit far-fetched to state as of now that the design of this experiment will yield the blueprint for a global network, it is logical to think -as of now- that the new internet will have similar structure and components to the classical one. Three basic components will be needed to put together a quantum network on the physical layer:

- **End-nodes:** these are the quantum computers, in whatever form they will exist. Probably calling them quantum computers is a bit of an overstatement as a simpler form like quantum processor (that can send and measure qubits) would suffice, since for most of the existing quantum communication protocols so far, processing a single qubit at a time is enough [1, 2, 3].
- **Switches:** in analogy to classical networks, some form of switch is needed to distribute and redirect the communication between channels. The switches avoid placing a quantum channel between each one of the nodes of the network.
- **Quantum repeaters:** this component also gets the name from its classical counterpart. Despite sharing the functionality (making sure that the signal is not lost during transmission), the mode of operation is completely different. Since quantum states cannot be copied faithfully, the signal cannot be regenerated after a certain propagation distance (like in a classical repeater). Through entanglement swapping, quantum information can be distributed without the need of signal regeneration.

This work focuses on last of the items and, more precisely, in a very concise operation that it carries out, the Bell State Measurement (BSM). To contextualize the bigger picture for the rest of this text, a detailed explanation on how a quantum repeater chain is envisioned is given in the following pages.

1.1 Repeater chains

The main goals of any communication protocol are two. First, security, i.e., the protocol must be secure against any possible attack that attempts to disclose the transmitted information. Second, usefulness; it must be possible to communicate by following the protocol. Having the latter without the former is not good enough as we want to keep our messages secret and private and, in case of intruders, detect their presence. There are many possible communication protocols that are both secure and useful, such as whispering, or signing. However, as the distances increase, one or the other has to be compromised because the signals that carry the information experience intrinsic attenuation. This was exemplified before by Alice loosing her confidence when she would try and run towards Bianca.

The goal of a repeater is to make sure that the information transmitted arrives at the destination in the best condition possible, ideally regardless of the distance. For that purpose, we will divide the communication distance in smaller segments named elementary links for which we can ensure that the information does not get lost and, by using the appropriate protocols, also secure. Simply by concatenating more elementary links, we will be able to cover the full distance. Up to this point the definition and use of repeaters is valid for both quantum and classical communications. However, there is a fundamental difference on how these two types operate.

A simplified chain of elementary links for classical communication consists of elements that receive the signal and regenerate it so that it can be forwarded to the next repeater, making the loss of information minimal. The reconstruction of classical information depends on creating a carrier signal resilient enough so that it can still be detected by the repeater element. Some attempts and novel ideas exist to implement this repeating-station for the quantum case [4, 5, 6, 7]. Here, we will focus on quantum repeater architectures [8] based on absorptive quantum memories – which store quantum states encoded into photons that are created elsewhere – and entangled photon-pair sources – which generate entangled states –, as depicted in figure 1a. A third element in 1a, the BSM, is responsible for implementing the entanglement swapping operation effectively concatenating the elements within and between elementary links. Moreover, it can herald which attempts yielded a successful entanglement swap.

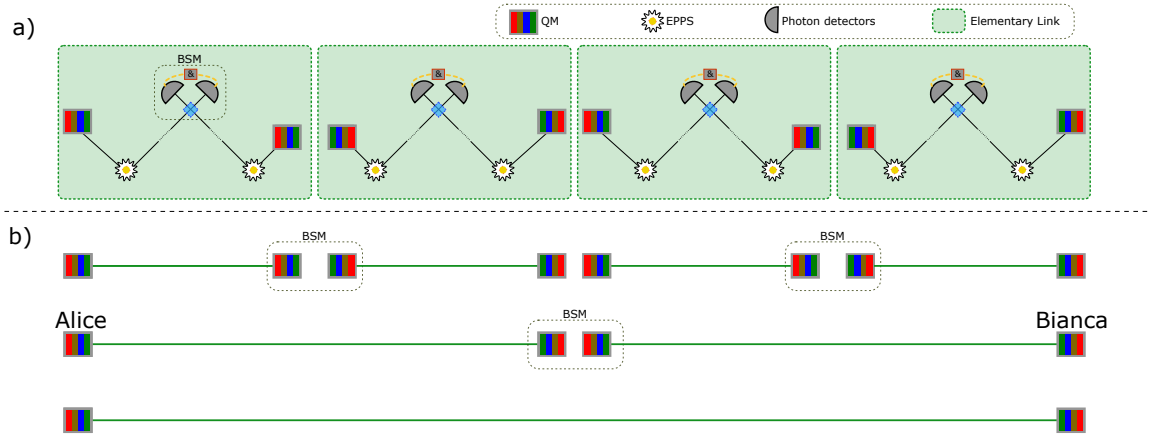

Figure 1: Schematics of memory based quantum repeater chain. In a, the different elements composing the elementary link are depicted. In b, we showcase, as we follow the protocol, the memories that share entanglement.

The entanglement swapping protocol that allows connecting multiple elements in the elementary link (quantum repeater) chain works in the folllowing way, as depicted in figure 1a: for both sides of the elementary link, entangled photon pairs will emerge from each of the entangled photon-pair sources (EPPS); while one is stored in one of the quantum memories, the other is transmitted (through a quantum channel) to a remote (distant) location where the BSM will be performed. The BSM consists in the projection of the joint quantum state of two photons (which, in this case, have not previously interacted) onto the Bell state basis. Uxpon a successful result, a set of unitary operations can be applied to the quantum states stored in the quantum memories such that entanglement between these two remaining states is established. Let us assume that we have distributed entanglement across our elementary links. It is noteworthy the role of the quantum memories: the elementary links in the chain will not necessarily establish entanglement synchronously. The presence of quantum memories combined with heralding of successful entanglement swapping operations, allows the temporal storage of entangled photons while other sections of the chain are still trying to distribute entanglement. Now, if we look at 1b, we only have to perform a set of BSM operations between adjacent memories to swap entanglement to the outer limits of our chain. For that, we will make use of our ability to pinpoint (thanks to heralding) the successful modes stored in the memories and perform the subsequent entanglement swapping operations only with those. In figure 1b, only the memories that are entangled with each other are depicted; they are connected with a green link. As the protocol progresses (going down in the figure), the memories that are entangled become more and more distant from each other. Once the chain is completed we can use this entanglement for any computing and/or communication protocol.

It is important to note how we have managed to cover a large distance without the need of sending a single photon across the entire chain. In this way, the transmitted quantum channels are not required to experience the transmission loss between end-nodes; however, they are still subject to the loss within each one of the elementary links.

1.2 Frequency multiplexed quantum repeater architecture

If everything were fields and flowers as that simple explanation we provided before, this thesis would not be needed but as we all know reality is never as simple. As previously mentioned, inefficiency of the components poses a limitation to the achievable throughput and/or distances covered by a quantum repeater chain. These come in two main forms: the loss in memory (out of the scope of this thesis) and the communication channel, which, in an optical fiber, are governed by the Beer-Lambert Law [9]; and a 50% maximum efficiency associated to the linear-optics-based BSM [1], which is in the core of the entanglement swapping protocol. In order to overcome these two forms of inefficiency, frequency multiplexing can be implemented in the quantum-repeater chain. The idea of multiplexing was already exemplified in the explanation of figure 1, in which the elementary links are concatenated using entangled states generated during different rounds (temporal multiplexing). For frequency multiplexing, instead of creating entangled photon-pairs that occupy a single spectral mode, a discrete collection of spectral modes is created such that the chance of at least one of them reaching the remote station after long-distance propagation and, then, producing a successful BSM, is increased, ideally up to 100%.

By implementing this extra layer, we can draw figure 2 of the frequency multiplexed elementary link. As we can see, it is composed by the same devices as in figure 1 but engineered to deal with many frequencies simultaneously. This new architecture is important for this work because it defines two types of BSMs. Both of them were also depicted in the more simplified version of the repeater chain but, once spectral multiplexing is added, a fundamental difference between them arises: on one hand, we have the remote BSM, within the elementary links; on the other, we have the local BSM, that concatenates adjacent elementary links. Since the former is distant from the sources, spanning the majority of the elementary link length, the propagation loss is significant (as it scales exponentially with distance); the latter, being local, does not suffer from this effect. Therefore, it is possible to formally define the probability of performing a successful BSM in these two cases, as follows:

$$P_{\text{remote}} = \eta_{\text{ch1}}\eta_{\text{ch2}}\eta_{\text{BSM}} = e^{-\alpha L/2}e^{-\alpha L/2}0.5 \tag{1}$$

$$P_{\text{local}} = \eta_{\text{BSM}} = 0.5, \tag{2}$$

where $\eta_{\text{ch1,2}}$ are the channel efficiencies for photons coming from either sources in the elementary link, η_{BSM} is the linear-optic-based BSM efficiency, L is the total elementary link length, and α is the fiber's loss coefficient, in [dB/km].

When one considers the multiple (n) discrete frequency modes emitted by the source in the frequency-multiplexed scenario, the probability of at least one frequency mode being successful in the remote BSM can be written as:

$$P_{\text{remote-mux}} = 1 - (1 - 0.5e^{-2\alpha L})^n, \tag{3}$$

effectively counteracting the detrimental exponential loss due to long-distance propagation in the fiber. In case the number of frequency modes can be increased significantly, close to deterministic entanglement swapping can be reached even for distances in the tens-of-kilometers range.

Very much like in the temporal multiplexing, when a spectral mode is successful in the remote BSM, all the other modes are discarded. Therefore, in order to achieve entanglement swapping between elementary links, the matching photonic quantum state previously stored in the quantum memory must

[1] Refer to section 3.3.1 for the mathematical derivation of this value.

be retrieved. Not only that, but a frequency-shifting operation is required so that modes stored and retrieved from adjacent elementary links are matched[2]. This is the role of the classical communication channel and of the frequency-shifting operation, both depicted in figure 2. After this operation, a single frequency mode interacts in the local BSM, which, thus, remains unchanged from the non-spectrally multiplexed case.

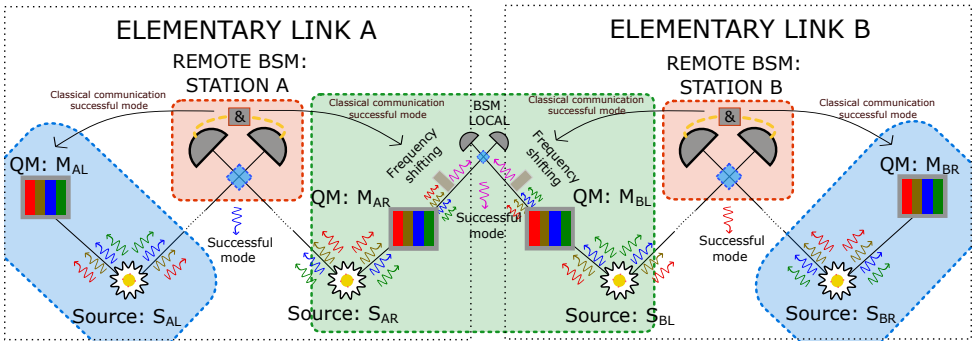

Figure 2: Depiction of two concatenated elementary links of a frequency-multiplexed quantum repeater. Elements in the same color-block are located together whereas the different blocks are at distant locations

In the drawing, we can see, in more detail, the different constituents of the frequency-multiplexed quantum repeater and a local BSM operation to concatenate elementary links. Although the reader now has an intuition on how it works, it is the goal of the following chapters to unveil the pieces to build such a quantum repeater and to explain in more detail how it works. Moreover the central piece of this project is regarding the frequency-multiplexed Bell-state measurement which will be explored in depth in the experimental section of the report.

Once the existence of quantum repeaters is argued necessary for a large scale quantum network, and their functionality is established, there's no other way but to start the road towards building one.

[2]A condition for the linear-optics-based BSM, as explained in Appendix C

A brief introduction to qubits and the encoding systems used in our lab will be our starting point that later will be used to carry out communication protocols.

2 Qubits and time-bin encoding

We will introduce the notion of qubit by going to the roots of quantum mechanics, to its initial postulates:

1. At each instant the state of a physical system is represented by a ket $|\varphi\rangle$ in the space of states that contains all there is to know about the system. Independent systems can be represented together by using the tensor product $|\varphi\rangle \otimes |\psi\rangle$
2. Every observable attribute of a physical system is described by an operator that acts on the kets that describe the system.
3. The only possible result of the measurement of an observable $\mathcal{A}$ is one of the eigenvalues of the corresponding operator $\hat{\mathcal{A}}$.
4. When a measurement of an observable $\mathcal{A}$ is made on a generic state $|\varphi\rangle$, the probability of obtaining an eigenvalue a_n is given by the square of the inner product of $|\varphi\rangle$ with the eigenstate $|a_n\rangle$, $|\langle a_n|\varphi\rangle|^2$.
5. Immediately after the measurement of an observable $\mathcal{A}$ has yielded a value a_n, the state of the system is the normalized eigenstate $|a_n\rangle$.
6. The time evolution of a quantum system preserves the normalization of the associated ket. The time evolution of the state of a quantum system is described by $|\varphi(t)\rangle = \hat{\mathcal{U}}(t, t_0)\,|\varphi(t_0)\rangle$, for some unitary operator $\hat{\mathcal{U}}$.

If we apply these concepts to a 2-level system, we obtain the formal definition of a qubit. Let us exemplify, using the postulates, what are: the qubit; the names given to the space we use; and the eigenvectors and eigenstates.

The qubit receives its name from its classical counterpart, the bit. Being the bit the simplest unit of information that can be processed by a computer, the qubit is the same for a quantum computer. Just like the bit can be in the states 0 and 1, the qubit can be written as a linear combination of the quantum states $|0\rangle$ and $|1\rangle$ that define our principal basis, the computational basis. The computational basis is associated to the observable Z, i.e., they are its eigenvectors, effectively defining the 2-level system. Given a qubit, if we apply the fourth postulate and *measure* in the Z-basis we obtain, as a result, one of its eigenvalues, associated to the basis on which the measurement was performed. The eigenvalues are 1 for the state $|0\rangle$ and -1 for $|1\rangle$, but a one-to-one mapping can be performed to associate the measurement results to classical bits 0 and 1.

Applying a unitary transformation $\hat{\mathcal{U}}$ such as described in postulate six, we can bring the quantum state from an eigenvector of the Z-basis to a general state like $\left(\alpha\,|0\rangle + \beta\,|1\rangle\right)$, a superposed quantum state. There are some superpositions which are more interesting than others: imagine we apply a transformation that brings the qubit to a state that has the same probability of measuring $|0\rangle$ or $|1\rangle$ when using the Z-basis. We define the states $|\pm\rangle = \frac{1}{\sqrt{2}}\left(\,|0\rangle \pm |1\rangle\,\right)$, which are the eigenvectors of the so-called X-basis; simultaneously, the vectors $|\pm i\rangle = \frac{1}{\sqrt{2}}\left(\,|0\rangle \pm i\,|1\rangle\,\right)$ are associated to the so-called Y-basis. One can prove that the eigenvalues of the new basis are the same given that the transformation is unitary.

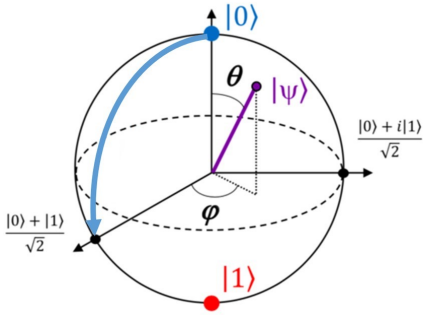

Figure 3: The Bloch sphere. The cardinal points representing the states $|0\rangle, |1\rangle, |+\rangle, |+i\rangle$ are marked. In purple an arbitrary state that can be defined by equation 6. In blue a unitary transformation that brings $|0\rangle$ to $|+\rangle$.

To exemplify how the measurements in different basis (or observables) work, we can think of the following examples. Imagine we have a qubit in the X-basis and we want to discover the probability of obtaining 0 while measuring on the Z-basis:

$$|\langle 0|+\rangle|^2 = \left|\langle 0| \cdot \frac{1}{\sqrt{2}}\Big(|0\rangle + |1\rangle\Big)\right|^2 = \left|\frac{1}{\sqrt{2}}\langle 0|0\rangle\right|^2 = \frac{1}{2} \quad (4)$$

We obtain a 50% probability to measure 0 and, therefore, also to measure 1. Once this measurement happens the fifth postulate applies. Note how our state could have been defined on the Z-basis and measured using the X-basis and we would have found the same results. Finally, note how if one measures a qubit in the basis that it was prepared, the result is deterministic, i.e., $|\langle -|-\rangle|^2 = 1$.

The three aforementioned bases (Z, X, Y) can be arranged in a geometrical structure called the Bloch-Sphere, which grants ease of visualization. The Bloch-sphere defines a surface which contains all possible states of a qubit; therefore, they can be depicted by a unitary vector from the origin to a point of the surface (purple vector in figure 3). Any point on the surface can be accessed by applying a unitary transformation that will conform a rotation of the vector defined between the point on the sphere and its center (blue curve in figure 3). On the cardinal points, we can find all six eigenvectors that define the three bases.

Although a unitary operation can be found to map a qubit state to any other, as previously mentioned, a remarkable theorem from quantum mechanics states that there is no single unitary transformation that maps any qubit to any other preserving the state of the first one. Formally (No-Cloning Theorem): Given $|\phi\rangle, |\theta\rangle$ arbitrary quantum states and $\hat{U}_c$, an arbitrary unitary operator such that:

$$|\phi\rangle \otimes |0\rangle \xrightarrow{\hat{U}} |\phi\rangle \otimes |\phi\rangle$$
$$|\theta\rangle \otimes |0\rangle \xrightarrow{\hat{U}} |\theta\rangle \otimes |\theta\rangle,$$

then $\langle\phi|\theta\rangle$ is 0 or 1, i.e., it is only possible if the states are the same or orthogonal.

2.1 Time-bin qubits

The formal definition of a qubit is an abstract mathematical object. When reality comes into play, many 2-level systems can be used or engineered to replicate the expected behaviour of qubits. The most famous ones are: the spin of an electron [10, 11]; the polarization of a photon [12]; or the charge/flux on a superconducting qubit chip [13]. Note that, for quantum communications, the qubits need to be transported between far locations. The use of optical photons as host particles to encode the qubit seems the most logical way to communicate, mainly for the speed at which it travels and the low attenuation (although not negligible) that it experiences through optical fibers.

In this experimental thesis, we will be working using time-bin qubits. The ideas behind time-bin qubit encoding

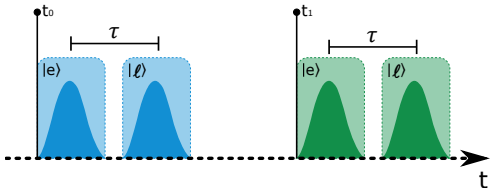

Figure 4: Time bins of two consecutive qubits (in different colors). We can see there is a time-window in which the photon (darker shade) is expected to be found. The first window is defined by a time reference whereas the second by a fixed delay τ from the first.

is simple to grasp, yet it comes at the expense of more complicated physical implementation. The 2-level system is defined given a reference on time for the first level, and a certain delay in which we may find the second level of the qubit. We can see in figure 4 how the bins are defined. This type of encoding is particularly useful when attempting to communicate over long distances: decoherence (loss of quantum information) of the qubits and chromatic dispersion on the quantum channels can be neglected and compensated in many cases [14].

Imagine we have an on-demand source of single photons that it is regularly pulsed. Along with each pulse we can already define our first time-bin: we will call it *early*, such that $|e\rangle \equiv |0\rangle$. With this definition, we have now a long time delay until the next qubit is defined (the difference between t_1 and t_0 in figure 4). We will make use of this time in between pulses to define a *late* time-bin $|\ell\rangle \equiv |1\rangle$, a second time-window after some time τ. Like this, we have completed the definition of the 2-level system we use for the Z-basis.

2.2 Beam-splitters: around the Bloch-Sphere

We have a way of defining the Z-basis for the qubits. However, we are still missing a way to implement unitary transformations that could bring us anywhere around the Bloch-sphere.

Although there is at least a couple of ways of implementing arbitrary time-bin qubits, we will use the initial proposal by [15]. Equation 5, is our starting point[3]. It describes a single photon input in an η beam-splitter (BS).

$$|\Psi_{out}\rangle = \left(U_{BS} a_{in}^{\dagger}\right) |0\rangle_a |0\rangle_b = \sqrt{\eta}\, |1\rangle_a |0\rangle_b + \sqrt{1-\eta}\, |0\rangle_a |1\rangle_b \tag{5}$$

The resulting state is in a superposition of the possible modes the input photon can take at the output. We connect each output to a different path length and we re-connect both of them to an optical switch. Note that, because both arms have different lengths, the photons will take a different amount of time to reach the switch. The difference in optical path is τ, hence defining our $|\ell\rangle$ bin in reference to the $|e\rangle$. The optical switch is operated letting through the expected photons at their arrival times, combining the qubit again in the same spatial mode. This way, we have managed to construct a superposed state starting from a Z-basis qubit.

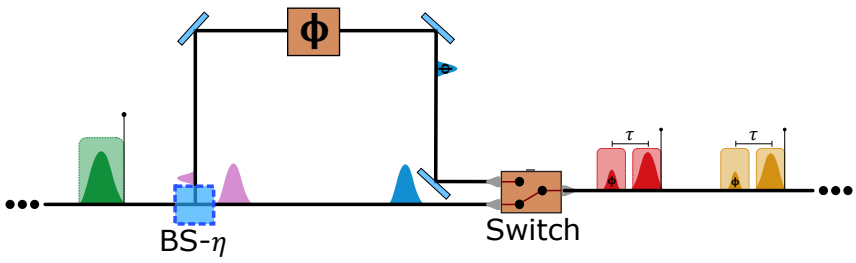

Figure 5: Pictorial representation of multiple qubits (different colors) undergoing the same unitary transformation. The coupling η and the applied phase Φ determine the qubit state.

Finally, we can add a phase-modulator in one of the arms; it will result in the possibility of accessing any point in the Bloch-sphere by properly combining the setting of η and ϕ. As we can see, equation 6 is a complete representation of any 1-qubit state on the Bloch-sphere. We can create any superposition by changing the coupling parameters η and the relative path between the arms.

$$|\Psi_{out}\rangle = \sqrt{\eta}\, |e\rangle + e^{i\phi}\sqrt{1-\eta}\, |\ell\rangle \tag{6}$$

[3]Visit AppendixB for derivation and notation

For practical reasons, and because some communication protocols have been proven secure in this condition, we can restrict the qubits to just Z- and X- basis instead of accessing all possible states. Like that, we can decide to fix the η BS to a 50:50 BS and ϕ such that the $|+\rangle$ and $|-\rangle$ states are created. Moreover, substituting the optical switch for another 50:50 BS at the expense of 50% loss of light allows to have only passive elements. The configuration with two BSs corresponds to a Mach-Zender interferometer, with output

$$|\Psi_{out}\rangle = \frac{1}{\sqrt{2}}\big(|e\rangle + e^{i\phi}\,|\ell\rangle \big);\ \phi \in [0, \pi]. \tag{7}$$

Creation of time-bin qubits using interferometers comes with two main consequences:

- There is a restriction on the duration of qubits τ combined with the repetition rate of the source to avoid time-bins from different qubits to mix or interfere at the beam-splitter.
- If one wants to create qubits on the Z-basis with this configuration, one needs to block one of the arms of the interferometer letting $|e\rangle$ or $|\ell\rangle$ through and increase the intensity of the light beforehand to compensate the loss.

2.3 Measurements

It is straightforward to realize that with the previously set configuration, the interferometers are performing a mapping onto the X-basis. By controlling the phase, mapping onto the Y-basis is also possible. Therefore, the same interferometers that create qubits can be used to measure such qubits in different bases. By placing detectors at the outputs of the interferemeter, a projective measurement onto these bases is performed. Creation and measurement of photonic time-bin qubits using interforemeters requires a stability of the phase. Inability to control the phase will impact crucially on the accuracy of the measurement. This thesis reports, in section 7.2.1, a more detailed explanation on the hows and whys of phase-stabilization.

2.4 Entangled states

A single qubit is already a powerful tool to exploit the properties of quantum mechanics applied to communications, but its applications are limited to quantum key distribution. Quantum computers consume resource in terms of entanglement and, in order to interconnect quantum computers, a quantum repeater must distribute entanglement. Entanglement leads to strong quantum correlations, which can be shared between two or more systems; it stems from the first postulate of quantum mechanics.

Even though more than two particles can be entangled, we will focus on the case of 2-particle entanglement since it exhibits a specific property named monogamy. Entanglement monogamy is referred to the specific type of entanglement in which the two qubits cannot be entangled to anything else; it is also said that the qubits are maximally entangled. These states are the so-called Bell-states and are the basis of any two-qubit state. These are denoted by:

$$\begin{aligned}
\big|\Phi^+\big\rangle &= \frac{1}{\sqrt{2}}\Big(|00\rangle + |11\rangle \Big);\\
\big|\Phi^-\big\rangle &= \frac{1}{\sqrt{2}}\Big(|00\rangle - |11\rangle \Big);\\
\big|\Psi^+\big\rangle &= \frac{1}{\sqrt{2}}\Big(|01\rangle + |10\rangle \Big);\\
\big|\Psi^-\big\rangle &= \frac{1}{\sqrt{2}}\Big(|01\rangle - |10\rangle \Big),
\end{aligned} \tag{8}$$

where the first number in each ket refers to one of the particles and the second, the other one.

The fine characteristic about entangled particles is that despite being two physically separate entities, they cannot be fully described by two separable quantum states.

$$\left|\Psi_{entangled}\right\rangle \neq |\phi_1\rangle \otimes |\phi_2\rangle$$

Therefore, they conform a single system as stated by the first postulate. That results in what some people refer as maximal coordination upon measurements: when one of the qubits is measured that will, following the fifth postulate, change the state and condition a measurement on the other qubit. The Bell states are the states onto which a BSM project. In the following sections, the mathematical formalism and applications of this measurement will be clarified.

The following section introduces several well-known general concepts used in the field of study. To help the reader, these concepts are surrounded by explanations of the BB84 and the MDI-QKD protocols. One will see that these concepts become relevant as the thesis progresses.

3 Quantum key distribution

The need to communicate with others in a public environment without disclosing the secret to any bypasser dates back more than 3000 years, and up to the present day, we are still in search for safer and faster communication protocols. Cryptography protocols are generally divided into two classes: private key and public key protocols. Before the advent of the RSA [16] public key protocol (named after its creators) in 1978, private key protocols, where only the sender and the receiver of the encoded message have access to the key, were the standard. It is straightforward to observe that the complexity involved in establishing a key only accessible to two parties to is the same as transmitting information that only two parties have access to, i.e., the key becomes the message. The obvious difference is that the key contains no information, and can be a random string of digits, so, if it is leaked to a third-party, no information is leaked with it.

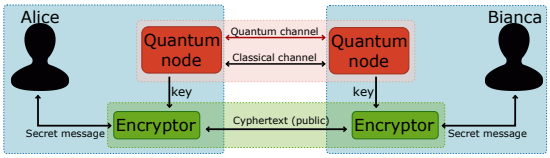

Figure 6: Secure communication application based on a QKD system: QKD establishes a secret key to be used by the encryptors (also decryptors). Once the message is encoded, it can be sent via classical public channels and only be deciphered by the other encryptor that holds the same key.

In 1917 Gilbert Vernam demonstrated a mathematical security proof of the so-called One-Time Pad cryptography protocol. In this protocol, the sender and the receiver share a perfectly random key that can be used once; the sender, then, performs a simple two-bit operation between the message and the key, transmits the resulting signal through a public channel, and the receiver performs the same operation between the received signal and the key to recover the original message. The requirement that the key can only be used once, by one of the parties, prevents widespread use of this protocol, as it poses a strong practical limitation. Quantum key distribution (QKD) offers, in theory, a secure way of distributing such keys granted by the laws of quantum mechanics. Once the key is established, the parties can communicate via a public channel using the One-Time Pad; a schematic of the whole protocol is presented in figure 6.

A number of QKD protocols have been proposed, in general, they feature the following characters:

- Alice, who wants to share some information with Bianca.
- Bianca, Alice's communication partner.
- Eve, an all-powerful eavesdropper, decided to spy on Bianca's and Alice's communication without being noticed.

As previously stated, the goal of any QKD protocol is to ensure that Alice and Bianca establish a random key that can be used for the One-Time Pad. Ideally, no information regarding the key is to be leaked to Eve, in which case it would be possible for the latter to tap into the communication and have access to the encoded message. Motivated by the No-Cloning Theorem, presented in the previous section, Bennett and Brassard developed the first QKD protocol in 1984.

3.1 The BB84 Protocol

Consider that Alice has access to a source of single photons and, by means of the interforemeter described in Section 2, she is able to encode quantum information in the temporal degree-of-freedom

of said photons, i.e., time-bin qubits. Everytime a single-photon is emitted from her source, Alice can choose (randomly) which basis is going to be used for time-bin encoding (Z- or X- basis) and its corresponding eigenstate ($|e\rangle$, $|\ell\rangle$ or $|+\rangle$, $|-\rangle$). Since two binary choices are required, the combination of the classical bits, a_i and b_i, determines the encoded quantum state, as seen in table 1.

	$a_i = 0$	$a_i = 1$
$b_i = 0$	$\|e\rangle$	$\|+\rangle$
$b_i = 1$	$\|\ell\rangle$	$\|-\rangle$

Table 1: The four possible states used in the BB84 protocol that Alice can generate, depending on the random bits a_i and b_i.

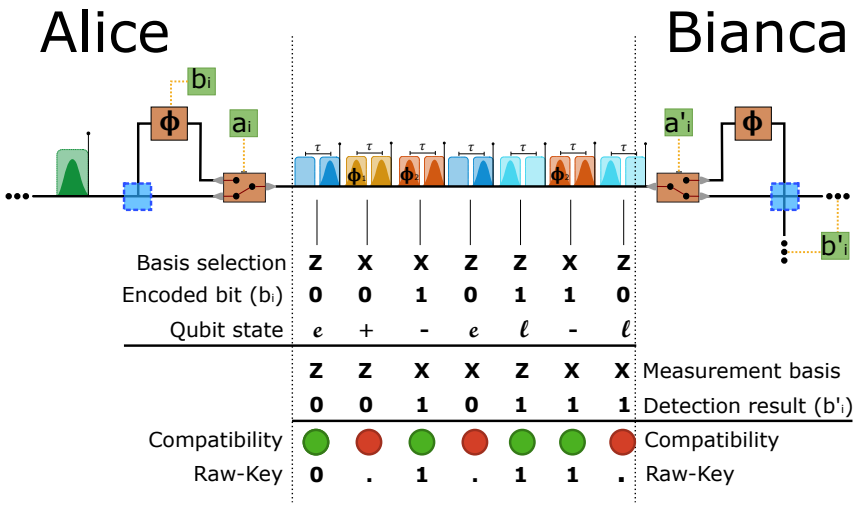

Figure 7: Steps of the BB84 protocol. In the top, the basis string used by Alice, the encoded bit and the corresponding sent qubit (according to table 1). On a second step, the bases Bianca used and her detection results. Finally, sifting yields some bits of raw-key.

After preparing her photonic qubit states, Alice sends them through a quantum channel (possibly an optical fiber) to Bianca, whose responsibility is to measure each of the incoming photons. In order to do so, she utilizes a measurement apparatus that is able to make projections of the time-bin qubit states onto the same bases used by Alice, i.e., Z- and X- basis; as previously discussed in Section 2, Biance employs, for measurement, an interferometer identical to the one Alice employed for state preparation, as depicted in figure 7 (with the addition of two detectors). The first part of the protocol (the quantum part), then, follows these steps:

- Alice sends $4n$ qubits, encoded at random, and records the strings of bits used for basis ($a = [a_0, a_1, a_2, ..., a_{4n}]$) and state selection($b = [b_0, b_1, b_2, ..., b_{4n}]$).
- Bianca projects the incoming photonic qubits onto randomly chosen bases, also recording the bit associated to the basis choice ($a' = [a'_0, a'_1, a'_2, ..., a'_{4n}]$) and the bit associated to the measurement result ($b' = [b'_0, b'_1, b'_2, ..., b'_{4n}]$).

After quantum state transmission and measurement is performed, Alice and Bianca are each in possession of two 4n-long strings of bits. They then turn to a classical public channel and announce to

each other (and to anyone else, including Eve) the string of bits corresponding to the basis choice. For those cases where Alice and Bianca used the same basis for both state preparation and measurement, they keep the bit associated to the state (prepared and measured, respectively). This step called *basis reconcilliation* or *key sifting* is necessary because, as demonstrated in equation 4, the result of a projective measurement onto a basis different than the one used for preparation yields a probabilistic outcome. Conversely, if the same bases are used, the outcome is deterministic, i.e., Alice's and Bianca's bits will be identical (provided there is no eavesdropper)[17]. It is important to note that only the information about the bases was disclosed publicly and not on the state preparation and measurement, which will be used as the final key.

Consider, now, the presence of Eve in the quantum channel and her attempt to extract information about the key shared by Alice and Bianca. Although many practical security breaches that could be exploited by Eve in her attempts have been found over the years for the BB84 protocol, assume ideal state preparation and measurement. The smartest strategy adopted by Eve would be to intercept the photons sent from Alice to Bianca, measure them, record the result, and relay them to Bianca. Since Eve has no access to the preparation basis used by Alice to encode her qubits, however, the measurement results will, as for Bianca, be either deterministic or probabilistic (on average half of the time each, since there are two possible preparation and measurement bases). Furthermore, Even will only have access to whether her result was one or the other during basis reconciliation between Alice and Bianca, by which time she would already have relayed the states to Bianca so that she can measure them not suspecting a man-in-the-middle.

The above analysis is important because it highlights the fact that, by intercepting and resending the quantum states, Eve is altering the conditions of the quantum channel specifically because she is unable to copy the states sent by Alice (keeping one and sending the other to Bianca) due to the No-Cloning theorem. Finally, the strength of the BB84 (and other QKD protocols), comes from the fact that, by sacrificing a subset of the bits after basis reconciliation, Alice and Bianca can estimate the quantum bit error rate (QBER) of their channel, i.e., the probability of incorrectly measuring a certain qubit provided that it has been sent. Based on the estimated QBER value, Alice and Bianca can detect the presence of Eve (with some certainty, which is diminished due to the presence of inherent noise in the system). In case Eve is detected, Alice and Bianca can choose not to use the key that had been previously shared, thus not compromising sensitive information. There are, also, protocols that allow to distill secure keys with a certain security threshold if the QBER is small enough; These are known as error correction protocols and privacy amplification [14]. Furthemore, it is important to note that the intercept-and-resend attack is not the best possible one [14], but common to all is the fact that Eve cannot extract information without increasing the QBER.

3.2 QKD Parameters

The No-Cloning Theorem is the basis of QKD and leads to the conclusion that, if an eavesdropper attempts to intercept the quantum state transfer that produces the key between the communicating parties, its presence will be detectable. However, it is only after the protocol has run its course that Alice and Bianca can estimate the channel parameters that allow them to extract the QBER and, finally, determine whether or not Eve acted. The estimation of the QBER is, thus, a core procedure during any QKD protocol. In the protocol utilized by Alice and Bianca so far, the photonic qubit states have no experimental imperfections and can be idealized as single-photons. In this scenario, the QBER is extracted in a straightforward way: consider that Alice and Bianca have, after basis reconciliation, a number n of shared bits; the measurements that were performed by both Bianca and Eve are, on average, different from the basis used by Alice half of the times, meaning that $\sim 2n$ quantum states have been transmitted; because of Eve's presence, the probability that an intercepted photonic qubit generates an error is, thus, 25% (50% $\times$ 50%); in conclusion, if Alice and Bianca sacrifice m bits (out of the n they

have), they will identify the presence of Eve (through the QBER) with a probability

$$P_{\text{eve}} = 1 - \left(\tfrac{3}{4}\right)^m. \tag{9}$$

In this idealized scenario, Alice and Bianca need only sacrifice a rather negligible amount of bits in order to consider their shared key secure within a robust certainty margin.

Unfortunately, deterministic single-photon sources with a high rate are not yet available; Alice and Bianca must, then, resort to practical photon sources that produce a photon-number distribution rather than a well-defined number state. This creates a security breach since Eve can, in principle, split the photons contained in a photonic qubit state prepared by Alice, hold on to one, and relay the remaining ones to Bianca. In this way, no cloning takes place, but Eve is able to access the qubit that was transmitted without being detectable in the QBER estimation. This strategy translates the so-called *photon-number splitting* attack [18], which creates the requirement of a robust estimation of the channel parameters taking into account the photon source used by Alice and its photon-number distribution: the **decoy-state** protocol [19].

In this protocol, Alice uses an imperfect source to encode qubits, but modulates the intensity of the pulses randomly, i.e., Eve has no access to the parameters associated to the photon-number distributions at each transmitted pulse. In general, and due to their availability and versatility, coherent sources (lasers) are employed as photon sources for decoy-state QKD; in this case, the photon-number distribution is Poissonian and the parameter used to describe the decoy-state protocol is the *mean-photon-number* μ[4]. Many different values of mean-photon-numbers can be employed for different compromises between accuracy of channel estimation and achievable rate, but we consider a three-state decoy protocol, where μ_v, μ_s and μ_d are used and refer to vacuum, signal, and decoy, respectively. After basis reconciliation, an extra round of communication between Alice and Bianca is necessary so that the mean-photon values associated with all the transmitted pulses is disclosed. This way, Alice and Bianca can extract the following parameters, provided that the source's photon-number distribution is known:

- **Yield (Y_n)**: The yield is the conditioned probability that a quantum state encoded into n photons is measured (in the same basis) by Bianca provided that it was emitted by Alice. It takes into account the intrinsic transmission loss across the quantum channel, the efficiency of the detectors employed by Bianca, and the presence of Eve.

- **Gain (Q_μ)**: The gain corresponds to the probability of extracting a bit of raw-key per transmitted pulse when the mean-photon-number μ is used. In other words, it is the Yield weighted by the probability of Alice emitting an n-photon pulse (this depends on μ_v, μ_s and μ_d).

- **Error rate (e_n)**: The error rate reflects the probability that a n-photon pulse detection extracts a wrong bit of key. It takes into account Bianca's detector's dark counts, the mismatch between bases, and Eve's presence.

- **QBER (E_μ)**: Finally, the QBER, as previously, is the probability of a pulse with a mean-photon-number μ yielding an incorrect bit of key provided the same basis was used for state preparation and measurement.

After estimation of each individual parameter, the following inequality can be written for the parameters S, the key generation rate, or number of successfully distributed bits per attempt [20]:

$$S \geq Q_\mu \Big\{ -H_2(E_\mu) + \Omega\Big[1 - H_2(e_1)\Big]\Big\}, \tag{10}$$

[4] See Appendix A

where Ω is the fraction of Bianca's detection that were due to Alice sending a single-photon state, e_1 is the error in the same case as before, and Q_{μ_s} and E_{μ_s} are the gain and QBER of the signal state; H_2 is the binary Shannon entropy [19]. The first term of the right-hand side of equation 10 is related to the amount of bits lost to error correction. The second term is associated to the total amount of raw-key that Alice and Bianca manage to produce. The final term is related to potential leaked information due to eavesdropping. Equation 10 not only provides a lower-bound for S but can only be positive if Eve's presence is not disruptive to the QKD section. Furthermore, it allows one to estimate the effect of different parameters on the key generation rate, including the distance that separates Alice and Bianca. It has been shown by theoretical and experimental realizations [21] that this distance cannot extend over a few hundred kilometers [22].

3.3 Measurement-Device-Independent Quantum Key Distribution

The decoy-state protocol enables a QKD session with imperfect single-photon sources, i.e., sources that produce photon-number distributions rather than deterministic single-photons, by circumventing the photon-number-splitting attack. Over the years, however, many other breaches have been discovered and exploited in the detection part of the QKD link; these breaches would allow Eve to extract information without being detected. The Measurement-Device-Independent QKD (MDI-QKD) protocol eliminates all the detector side-channel attacks by combining the decoy-state protocol with an architecture that allows delegating the measurement to an non-trusted third-party (other than Alice and Bianca), usually called Charlie.

In this scenario, both Alice and Bianca prepare and send states in the same fashion as described for Alice in the BB84 protocol; but instead of sending states one to the other, they both send them to Charlie, which is placed in between – refer to figure 8. The security of the protocol is due to the nature of the measurement performed by Charlie: a Bell-State Measurement (BSM). For this measurement, the joint-states of the photonic qubits prepared by Alice and Bianca are projected on the Bell-basis (the states presented in equation 8); after a successful BSM, Charlie discloses the output state information.

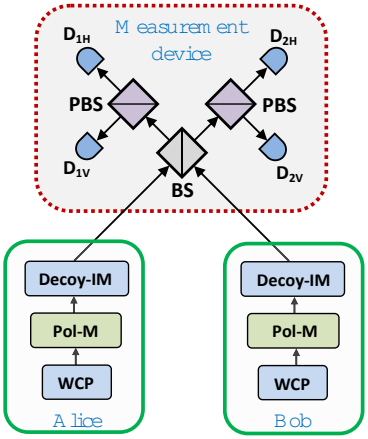

Figure 8: First proposal of MDI-QKD schematics by [2], using polarization qubits and decoy states.

Even though the states are not previously correlated, a successful joint projection onto the Bell-basis allows Alice and Bianca to establish a key: in possession of the Bell-state projection information, one can only determine unambiguously which states were prepared with information of at least one of them, i.e., information that only either Alice or Bianca have, since they were the ones that prepared the states. The MDI-QKD protocol uses the properties of entanglement to ensure the distribution of key. However, instead of generating entangled particles and distributing them, independent pulses of light are projected onto a Bell state in a remote station; one could think of this as a time-reversed entanglement distribution protocol. Note that there is no assumption that Charlie actually performs a BSM; she has all control about her station. However, any attempt from her side to learn more about the states she receives would yield errors on the BSM projections, increasing the QBER and effectively making her visible or denying service of communication between Alice and Bianca.

3.3.1 Bell-state measurement

A Bell-state measurement, as discussed before, is a projective measurement of any bipartite qubit state onto the Bell basis, composed of the four maximally-entangled Bell states. As will be discussed in

the following section, this operation is not only at the heart of the MDI-QKD protocol but also of the quantum teleportation and entanglement swapping operations and hence the quantum repeater. It is also the focus of this thesis, since the possibility of performing a frequency-multiplexed BSM is the goal of the project.

It is interesting to observe that a BSM can be easily performed in a quantum computer through a C-NOT gate between the two input states followed by X-basis measurements. The states sent by Alice and Bianca, however, are photonic qubits, i.e., the quantum information is encoded in the degree of freedom of optical photons, which are not directly compatible with a quantum computer. Fortunately, one can harness the photon-bunching effect when two indistinguishable photonic wave-packets are directed to a symmetric beamsplitter in order to implement a so-called linear-optics-based BSM (LO-BSM). This alternative comes with a limitation in the achievable efficiency: consider that a LO-BSM receives, at its inputs, the four Bell-states; the detection patterns at the detectors connected to the output of the beamsplitter can be found to be

$$\begin{aligned} \left|\Phi^{+}\right\rangle &= \left((a_e^\dagger)_{in}(b_e^\dagger)_{in} + (a_l^\dagger)_{in}(b_l^\dagger)_{in}\right)\left|0\right\rangle_a\left|0\right\rangle_b \\ &\xrightarrow{BS} \frac{1}{2\sqrt{2}}\left[(a_e^\dagger)^2 - (b_e^\dagger)^2 + (a_l^\dagger)^2 - (b_l^\dagger)^2\right]\left|0\right\rangle_a\left|0\right\rangle_b; \end{aligned} \tag{11}$$

$$\begin{aligned} \left|\Phi^{-}\right\rangle &= \left((a_e^\dagger)_{in}(b_e^\dagger)_{in} - (a_l^\dagger)_{in}(b_l^\dagger)_{in}\right)\left|0\right\rangle_a\left|0\right\rangle_b \\ &\xrightarrow{BS} \frac{1}{2\sqrt{2}}\left[(a_e^\dagger)^2 - (b_e^\dagger)^2 - (a_l^\dagger)^2 + (b_l^\dagger)^2\right]\left|0\right\rangle_a\left|0\right\rangle_b; \end{aligned} \tag{12}$$

$$\left|\Psi^{+}\right\rangle = \left((a_e^\dagger)_{in}(b_l^\dagger)_{in} + (a_l^\dagger)_{in}(b_e^\dagger)_{in}\right)\left|0\right\rangle_a\left|0\right\rangle_b \xrightarrow{BS} \frac{1}{\sqrt{2}}\left[a_e^\dagger a_l^\dagger - b_e^\dagger b_l^\dagger\right]\left|0\right\rangle_a\left|0\right\rangle_b; \tag{13}$$

$$\left|\Psi^{-}\right\rangle = \left((a_e^\dagger)_{in}(b_l^\dagger)_{in} - (a_l^\dagger)_{in}(b_e^\dagger)_{in}\right)\left|0\right\rangle_a\left|0\right\rangle_b \xrightarrow{BS} \frac{1}{\sqrt{2}}\left[a_l^\dagger b_e^\dagger - a_e^\dagger b_l^\dagger\right]\left|0\right\rangle_a\left|0\right\rangle_b, \tag{14}$$

where $a^\dagger$ and $b^\dagger$ are the creation operators associated to both output spatial modes of the beam-splitter and the subscripts e and l refer to time-bins early and late, respectively. As can be seen, the states $|\Phi\rangle^{\pm}$ produce ambiguous detection patterns and, thus, cannot be distinguished. However, states $|\Psi\rangle^{\pm}$ produce unambiguous detection patterns, yielding an overall LO-BSM efficiency of 50%.

There is a number of theoretical proposals that would allow breaking the degeneracy (the one of $|\Phi^{+}\rangle$ and $|\Phi^{-}\rangle$) of the LO-BSM and, thus, increase the efficiency of the measurement. These proposals involve: using hyper-entanglement to extend the correlations to a higher dimensional Hilbert space and make use of correlations of entanglement in that dimension [23]; the use of ancillary qubits to gradually increase the efficiency [24]; or the use of non-linear crystals to condition interaction based on the quantum information [25]. All of the above report, theoretically, a more than a 50% efficiency and even an achievable 100% efficiency for the latter. Physical implementation, however, is extremely complex and, up to this day, has not been demonstrated with reasonable rates.

QKD is one of the simplest forms of quantum communication. We used this framework to showcase how qubits can be generated and measured to obtain a secret key, what the presence of intruders does to our communication and how can we model the throughput of these protocols. Moreover we presented a BSM and discussed its implementation and limitations.

As of now, we have gone many most of the basic tools of quantum communication. It is time to move to more complicated quantum communication protocols and start putting together the pieces that, at first, may seem totally unrelated, in order to build a quantum repeater.

4 From QKD to quantum repeaters

The driving force of the quantum repeater technology is the possibility to distribute quantum information over arbitrarily large distances, effectively beating what is known as the repeaterless bound. This bound is imposed by the channel loss, which, even though small, scales exponentially.

4.1 Entanglement swapping

Quantum teleportation (figure 9) is an operation by which a quantum state can be transferred between parties that share an entangled state. Assume Alice has a qubit she wants to transfer to Bianca. A third party, Charlie, creates and distributes Bell states encoded into optical photons to Alice and Bianca. The protocol works as follows

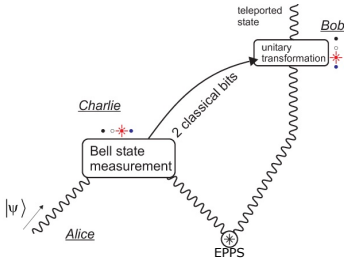

Figure 9: Quantum teleportation. Distance on the horizontal axis and time on the vertical. Undulated lines represent quantum information and the solid line classical communication. The source emits maximally entangled states. Figure from [26].

- In a first step Charlie sends one of the photons of the Bell state to Bianca and the other to Alice. Note how Alice and Bianca can be as far apart as they want, as long as they are in reach with Charlie.
- Upon receiving the photon from Charlie, Alice projects the joint state of the quantum state to be transferred and that of Charlie's onto a Bell state, effectively performing a BSM.
- If successful (as there are also inefficiencies associated to such measurements), she can communicate her results to Bianca over a classical channel. Depending on the information received, Bianca performs a predetermined unitary transformation on the state she received from Charlie in order the reconstruct the quantum state Alice wanted to transfer.

Formally, the protocol can be described as follows. The states of the photons involved are: an arbitrary qubit to be teleported $|\phi_A\rangle$; and the Bell state $\left|\Phi^-_{A',B}\right\rangle$, where the subscripts are associated with Alice (A, A') and Bianca (B). The three particle joint state reads:

$$\left|\Pi_{A,A',B}\right\rangle = |\phi_A\rangle \otimes \left|\Phi^+_{A',B}\right\rangle = \frac{\alpha}{\sqrt{2}}\Big\{\,|0_A 0_{A'} 0_B\rangle - |0_A 1_{A'} 1_B\rangle\,\Big\} + \frac{\beta}{\sqrt{2}}\Big\{\,|1_A 0_{A'} 0_B\rangle - |1_A 1_{A'} 1_B\rangle\,\Big\} \tag{15}$$

It can be rearranged as

$$\begin{aligned}\left|\Pi_{A,A',B}\right\rangle = \frac{\alpha}{2}\Big\{ &\left|\Phi^+_{A,A'}\right\rangle \otimes (\alpha\,|0_B\rangle - \beta\,|1_B\rangle\,) \\ &+ \left|\Phi^-_{A,A'}\right\rangle \otimes (\alpha\,|0_B\rangle + \beta\,|1_B\rangle\,) \\ &+ \left|\Psi^+_{A,A'}\right\rangle \otimes (\alpha\,|1_B\rangle + \beta\,|0_B\rangle\,) \\ &+ \left|\Psi^-_{A,A'}\right\rangle \otimes (\alpha\,|1_B\rangle - \beta\,|0_B\rangle\,)\Big\}\end{aligned} \tag{16}$$

The result indicates that, after a projection onto the Bell basis by Alice, the quantum state of the photon in Bianca's possession will require a unitary transformation to recover Alice's input state. Fortunately, Bianca knows exactly which transformation to perform given the result of the BSM. It is also noteworthy that no party involved in the transfer of $|\phi\rangle$ from Alice to Bianca had access to the actual quantum state (except for Alice, who created it).

We have portrayed a basic teleportation setup. What would happen if the qubit to be teleported was entangled with another particle as in figure 10. In this case, there is initial entanglement between the pairs [A,B] and [C,D]. Qubits B and C are sent to a central station, and projected onto a Bell state. If said measurement is successful, we end up with particles A and D, which, after a unitary operation dependent on the measurement outcome, become entangled, even though they never interacted. This is called entanglement swapping.

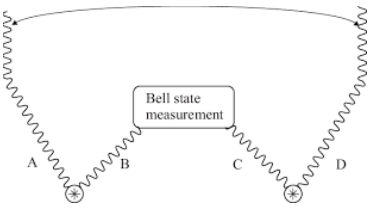

Figure 10: Entanglement swapping operation. The entanglement shared between the pairs of photons [A,B] and [C,D] is teleported to the pair [A,D] upon a successful Bell-state measurement. Distance in the horizontal axis and time on the vertical. Picture taken from [27].

4.2 Quantum relays and repeaters

The operation of entanglement swapping is the key ingredient for quantum repeaters. As we can see the result is two entangled particles that never interacted and moreover, if distances are taken into account: supposing the repeaterless bound to be L. Particles B and C can travel L towards the central station, meaning the sources they were emitted from can be $2L$ from each other. Also, A and D can travel in opposite direction such that in the end A and D cover a distance of $4L$.

If we were to implement a second BSM station where particle D is with another entangled pair, we could extend that distance again by $2L$, reaching $6L$ between A and one of the new particles. We can see how this configuration allows us to extend arbitrarily the distance we cover by adding more and more entangled photon pair sources and their corresponding Bell-state measurement stations, forming a chain. The protocol explained in the previous section can be extended to a chain, in which bi-partite entanglement can be distributed to arbitrarily distant parties. By concatenating entangled photon pair sources and BSMs, long distances can be covered since the photons are not requiered to travel farther than the repeaterless bound.

The architecture previously described is known as a quantum relay. Despite having the ability to entanglement swap and, therefore, distribute entanglement above the repeaterless bound, it is not practical: loss and BSM inefficiency render the chances of having multiple, synchronous and successful entanglement swapping operations to zero. To complement the quantum relay and elevate it to the status of **quantum repeater**, we make use of quantum memories with the feed-forward capabilities that were explained in the Introduction. Just like that, we can overcome the inefficiency of the entire chain by reducing it to the smaller sections, whose efficiency can be increased by spectral-multiplexing and the BSM for concatenation. In fact, this realization leads to the concept of the elementary link, the minimum cell of the quantum repeater chain, which contains the building blocks of the architecture: two EPPS, two quantum memories (QM), one BSM station and both classical and quantum information channels.

The previous section finished with the blueprint for a repeater chain. In this following section we will see how to get that idea and bring it to a reality, discussing the specific details and parts. It also revisits the concept of frequency multiplexing and then focuses on frequency-multiplexed quantum repeater architecture.

5 Frequency-multiplexed quantum-repeater architecture

The motivations for multiplexing were explained in the introductory part of the text: it is a mean of overcoming losses in the channels and the inefficiency of the BSM. Even though different technologies allow different degrees and types of multiplexing (spatial [28], temporal [29] and frequency [8] being the usual). All of them satisfy equation 3 and can be employed simultaneously. In this thesis we mainly study the frequency-multiplexed quantum repeater architecture and its blueprint can be seen in figure 11.

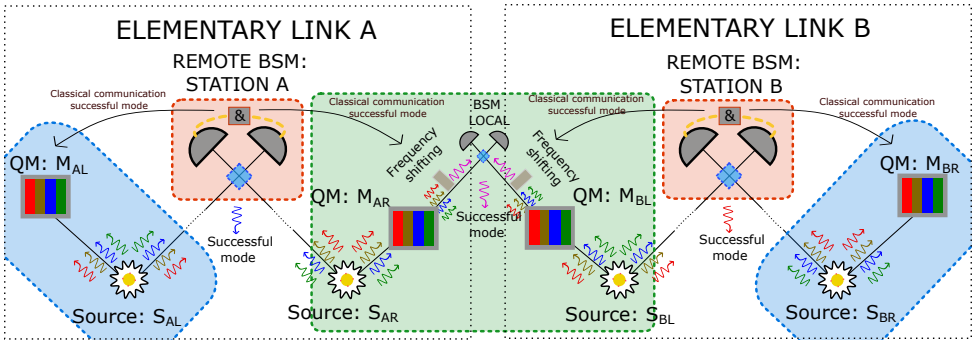

Figure 11: Schematics of frequency-multiplexed quantum-repeater architecture

In a single attempt to establish entanglement between the two nodes of an elementary link A, the entangled photon-pair shources (EPPS) S_{AR} and S_{AL} will emit maximally entangled Bell states in many frequencies or spectral modes (depicted by different colors). One of the photons of each pair travels towards the remote BSM, and the other towards the quantum memories (QM) M_{AR} and M_{AL}, where the quantum state will be stored. When the photons reach the remote BSM stations, each spectral mode will be subjected to a BSM. If this operation is successful for at least one of the frequencies (spectral mode blue for elementary link A) entanglement swapping to the corresponding spectral modes stored in the QMs takes place. Exactly the same procedure happens for the elements in elementary link B, where the successful mode is red.

At this point, another entanglement swapping step entangles photons in the far-edge QMs M_{AL} and M_{BR}. For this to happen, however, the photons must be indistinguishable in the local BSM. Statistically, and as depicted in figure 11, this is unlikely, and the successful spectral modes from different elementary links will not be matched. It is thus necessary to map them to a common spectral mode. That is the purpose of the frequency-shifting operation, which requires the information from the remote BSM. After shifting and filtering, photons emerging from adjacent elementary links will be indistinguishable in all degrees of freedom (since spatial mode, temporal mode, and polarization mode are already matched). The local BSM is thus not multiplexed, and will have an efficiency limited by the linear-optics-based setup; if this final entanglement swapping operation is successful, QMs M_{AL} and M_{BR} will share entanglement.

In the following subsections, the individual building blocks of the FM-QRA depicted in figure 11 will be analyzed more deeply, namely the entangled photon-pair sources, the absorptive quantum memories,

and the frequency-shifting and filtering stations. Since the frequency-multiplexed BSM is the focus of this thesis, a more complete analysis is presented in the next section.

5.1 Entangled photon pair source

A fundamental tool in building a quantum repeater is the entangled photon-pair source (EPPS). Due to its versatility, especially in terms of frequency-multiplexing, we opt in the context of a frequency-multiplexed quantum repeater for EPPSs based on Spontaneous Parametric Down Conversion (SPDC). SPDC is a non-linear optical process that enables the creation of two photons based on the annihilation of a so-called pump photon. The process requires two conditions (energy and momentum conservation) to hold in a crystal exhibiting second-order susceptibility non-linearity. The Hamiltonian of the SPDC process can be shown to yield, up to a first-order approximation, a time-evolution operator (according to the sixth postulate of quantum mechanics, as presented in the Introduction) that corresponds to the well-known *squeezing* operator [30], of the form:

$$\hat{S}(t) = e^{\xi t \hat{a}_s^\dagger \hat{a}_i^\dagger - \xi^* t \hat{a}_s \hat{a}_i}, \tag{17}$$

where ξ is a coefficient that depends on the electric field amplitude of the pump beam, and the subscripts s, i are associated with the two output fields, historically dubbed *signal* and *idler*.

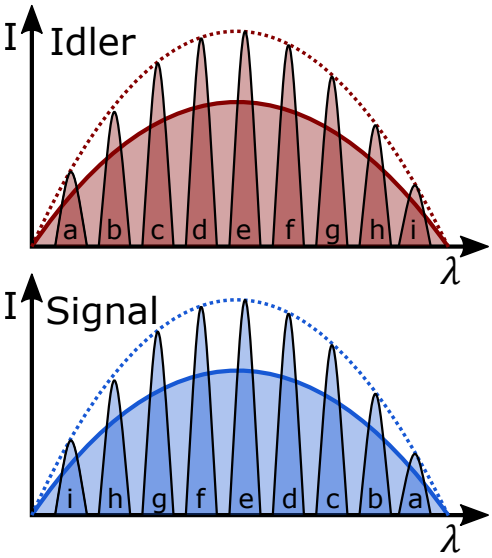

Figure 12: Depiction of the spectral emission of the source on the idler and signal regions. With no cavity (big colored area) and with cavity (defined spectral modes). With letters we have tagged the modes that are created together by conservation of energy

By designing a crystal with the correct parameters, a pump at $523.5nm$ can generate signal and idler beams at $795nm$ and $1532nm$ wavelengths that match: (i) the optical transition of the employed absorptive quantum memories, based on Tm; and, (ii) the minimum attenuation in optical fiber propagation. Moreover, it can be shown that, if the pump beam is cast into a superposition, for instance an X-basis time-bin $|\varphi\rangle_p = \frac{1}{\sqrt{2}}\left(|e\rangle_p \pm |\ell\rangle_p\right)$, the output state will, considering the annihilation of a single pump photon, be the maximally entangled state

$$|\Phi^\pm\rangle = \frac{1}{\sqrt{2}}\left(|e,e\rangle_{s,i} \pm |\ell,\ell\rangle_{s,i}\right). \tag{18}$$

Separation between signal and idler photons can be performed with a wavelength demultiplexer (such as a dichroic mirror), so that they can be collected individually and directed either to the quantum memory or to the remote BSM through a long fiber.

Due to the broadness of the output spectrum of an SPDC source (that stems from both the short length of the employed non-linear crystal and the broad pump spectrum [31]) it can be engineered into a discrete set of narrow spectral modes. One solution is post-filtering, i.e., using an optical cavity to filter the output allowing only the spectral modes of interest to be transmitted. Due to the energy conservation requirement, signal photons in specific spectral modes will be correlated (ideally, entangled) with idler photons occupying a corresponding spectral modes. Although effective, this solution has the drawback of wasting spectral power density after the SPDC process takes place, since the cavity will filter unwanted modes. In other words, very high pump intensity is required to create pairs with a reasonable effieciency within a small spectral window. A way to overcome this limitation is to embed the

SPDC crystal within a cavity, such that the spectral power density of the output states is concentrated in the allowed modes. Figure 12 depicts possible output spectra from cavity-embedded SPDC sources; such a source has been designed to produce spectral modes separated by $6GHz$ with a bandwidth of $700MHz$ [32].

5.2 Absorptive quantum memories with fixed storage time

The quantum repeater architecture introduced above requires heralding of a successful entanglement swapping operation across an elementary link. That happens only after a certain time from the creation of the entangled photon-pairs in the source, since the BSM station is distant from the nodes of the elementary link. It is straightforward to show that the time necessary for the photon to traverse the distance between either nodes and the BSM station and, afterward, for the measurement information to propagate back to the nodes is $t = \frac{L}{c}$, where L is the node-to-node length of the elementary link. It is, thus, necessary for the remaining photon of the generated pair to be stored efficiently during this time so that, afterwards, and assuming a successful BSM result, it can be used to perform subsequent operations.

Absorptive quantum memories based on rare-earth-ion-doped crystals are the candidates of choice for implementation of a frequency-multiplexed quantum repeater since they offer broad inhomogeneous broadening of the optical transition and long-coherence times that can match elementary link lengths up to tens of kilometers [33]. A well suited quantum memory protocol is the atomic frequency comb (AFC) protocol, which involves the selective optical pumping of ions into a shelving level with a certain periodicity to engineer a so-called atomic frequency comb. Upon absorption, the joint state of the ensemble is cast into a Dicke state [33]; the collective excitation rephases at a time inversely proportional to the engineered periodicity of the created comb [33]. This way, a fixed storage time that corresponds to the time necessary for the information sent from the BSM station to arrive at the elementary link node is programmed into the quantum memory.

5.3 Frequency shifting station

Frequency-multiplexing is only possible if the frequency modes simultaneously stored in the quantum memories can be accessed individually. This follows from the previously mentioned observation that, in the frequency-multiplexed BSM, all the modes will be discarded except for the one that yielded a successful BSM result. Concatenation of multiple elementary links then relies on the efficient mapping of the successful mode onto the desired – previously agreed upon – mode. This last step guarantees that the local BSM can be performed between modes emerging from two adjacent elementary links.

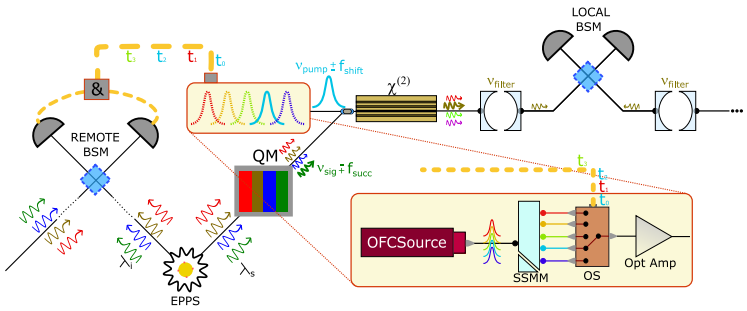

Figure 13: Proposal [32] for the frequency conversion station. A bank of frequency modes is prepared (by frequency-shifting ν_{pump}). Each one will induce an slightly different quantum frequency conversion of the memory-retrieved photons, effectively selecting the desired one (correlated with the successful mode in the remote BSM) after spectral filtering. The conversion takes place in a non-linear crystal.

Following figure 13, the information about which spectral mode produced a successful BSM result is sent to the QM. At this point, the photonic qubits previously stored are reemitted from the QM and, in the solution proposed in [32], are directed to a non-linear crystal. There, they interact with a strong pump beam whose center wavelength can be shifted and selected such that it conforms with the following frequency relation:

$$\left(\nu_{pump} \pm f_{shift}\right) \pm \left(\nu_{signal} \mp f_{success}\right) = \nu_{filter}, \tag{19}$$

where ν_{filter} is the previously agreed upon optical frequency mode common to the elementary links; $f_{success}$ is the frequency shift of the successful frequency mode on the remote BSM relative to ν_{signal}, the central spectral mode emitted by the EPPS; and f_{shift} is the corresponding frequency shift imposed onto ν_{pump}. To select the spectral mode that will be used as pump, a reservoir of possible pumps is at disposal to be sent through the crystal. An optical cavity aligned to ν_{filter} ensures that only the spectral mode of interest is directed to the local BSM. This process is called feed-forward spectral mode-mapping (FFSMM), since the spectral modes are shifted based on the information received from the remote BSM.

With this section the more formal and theoretical introduction to the topic finishes. We have exemplified and showcased most of the tools needed to understand the concept of frequency-multiplexed quantum repeater architecture, why is it needed, what it does and how it can be used. The following part of the thesis takes on a more experimental approach starting with the problem of demultiplexing of a frequency-multiplexed BSM; and culminating with experimental results.

In this section we dive into the core of the thesis. We report the chosen SSMM for frequency-demultiplexing and explain its characteristics and expected results.

6 Demultiplexing the BSM: theory and simulation

As previously mentioned, it is crucial for the operation of the frequency-multiplexed quantum repeater that one can identify which spectral mode yielded a successful BSM result. For that purpose, spectral demultiplexing is required. In order to reduce the complexity of the experimental setup, we choose to perform such demultiplexing after the multiple frequency modes interacted in the BSM's beamsplitter. In our case, demultiplexing maps spectral modes onto spatial modes. Hence, even though only a single beamsplitter is necessary, an array of single-photon detectors after the beamsplitter is required. This way, detections in specific single-photon detectors are associated with the corresponding spectral mode.

6.1 Virtually Imaged Phased Array (VIPA)

Due to the nature of the demultiplexing operation considered here, it will henceforth be dubbed spectral-to-spatial mode mapping (SSMM). In general, SSMM can be achieved in the optical domain by employing the mechanism of chromatic dispersion, whereby different wavelengths (thus, different spectral modes) experience differente indices of refraction when propagating through a given material: an example of this technology is a prism. The spectral resolution, or capacity of distinguishing between two adjacent spectral modes, of a prism, however, is limited to several nanometers. Another technology, which allows for finer spectral resolution, is the Bragg grating, where a periodic structure is created and the periodicity allows filtering a specific spectral mode. By concatenating several of these structures, multiple spectral modes can be mapped onto different spatial modes. An example of this technology are free-space Bragg-gratings and Fiber Bragg gratings. While the former has already been put into practice in [34] for similar purposes with a spectral resolution of $\sim 20GHz$, the former can reach spectral resolutions in the order of hundreds of MHz. Such devices, become severely inneficient if the number of spectral modes increases and, by conseguence, also the number of concatenated structures.

Finally, arrayed waveguide gratings (AWG), which function based on the constructive/destructive interference of different spectral modes that acquire incremental phases while propagating through waveguides of slightly different lengths, can also be employed for SSMM. An example are commercially available wavelength division multiplexers (WDMs), which, offer the ability to distinguish adjacent spectral modes at a spectral distance of $\approx 22GHz$ at $1550nm$ with reasonable ($\sim 6dB$) insertion loss.

Since the strength of the frequency-multiplexed quantum repeater architecture lies in how extensive the multiplexing can be, our goal is to push the spectral resolution of the SSMM solution as much as possible. The previously mentioned ones, even though well established, are limited either by loss (in case of fiber Bragg gratings) or by the resolution itself, in the range of GHz. A device called Virtual Imaged Phased Array, or VIPA, for short, is extremely interesting for our application as it achieves MHz-range spectral resolution and theoretical loss in the range of $2dB$ [35] while dealing with multiple spectral modes.

6.1.1 Physical appearance

In figure 14, the VIPA is presented in comparison with a typical etalon cavity. As we can see, the design is rather similar: both have two parallel reflection-coated surfaces such that the beam of light bounces between one and the other. The main difference is that one of the surfaces of the VIPA is

completely reflective (R) and has a small opening into which the input light beam should be directed, while the other is partially reflective (r); this is in contrast with the etalon cavity, where the coating is homogeneous across both surfaces. The result is that no spectral modes are reflected by the VIPA, as is the case for the Etalon cavity.

The devices considered in our experimental implementation were chosen such that the reflective coatings are matched for the optical telecommunication C and L bands, with $R \approx 1$ and $r \approx 0.95$. They are $t = 1.686mm$ thick and are based on fused silica, with an index of refraction $n = 1.46$. The physical dimensions of the device, as well as the reflection coefficient of the coatings and the index of refraction of the bulk material, will define its spectral properties, which will be discussed further on.

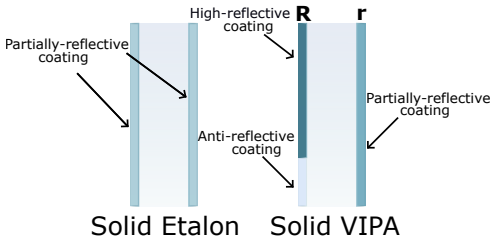

Figure 14: Etalon cavity (left), for comparison, and VIPA (right).

6.1.2 Operation and behaviour

The main characteristics of the light that outputs the VIPA we are interested in are: spectral power density, spectral/spatial resolution of adjacent spectral modes, and cross-talk. These are determined by the physical parameters of the VIPA and of the input light (spatial mode, focal point, beam waist, and incident angle).

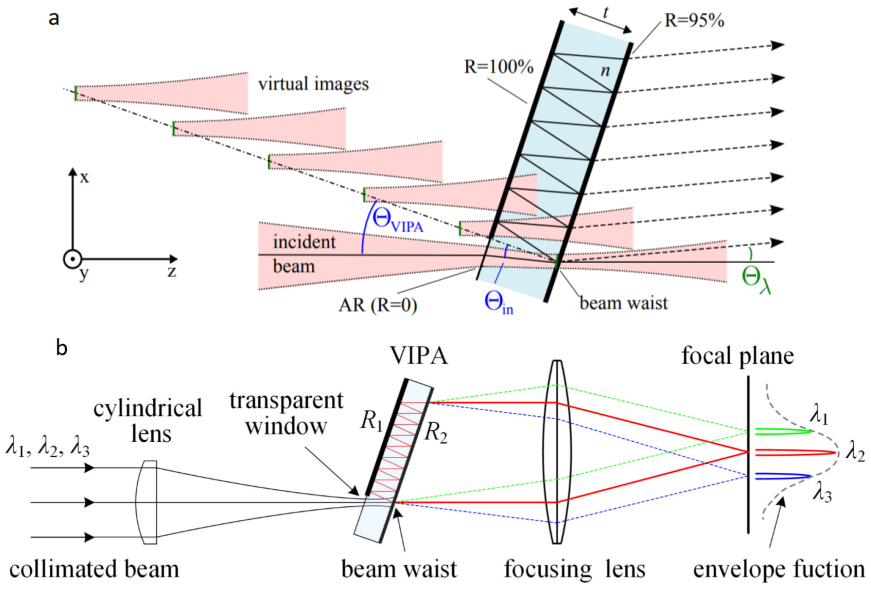

Figure 15: Principles of the VIPA. In a, an input beam of wavelength λ is coupled to the VIPA and generates the array of virtual images that emit at an angle θ_λ. In b, the VIPA in its working setup with the coupling and focusing lenses. Three wavelengths are demultiplexed as they output at different angles. Picture extracted from [36]

Consider a collimated beam of light containing multiple spectral modes that impinges on a cylindrical lens; the output beam will be focused on one transverse spatial coordinate (say, $\hat{x}$), giving the spatial profile of the beam an ellipsoidal shape. The position of the back surface of the VIPA (the one coated

with r) is chosen such as to match the focal point of the cylindrical lens and such that the beam hits the opening of the front surface (the small anti-reflective coated region coated, see figure 15b). As the beam propagates, it will transmit through the back surface with a rate $1 - r$; since r is close to unity, the majority of the optical power will reflect off forming an angle $2\Theta_{\text{in}}$ with respect to the incident beam.

If the incident angle is correctly adjusted, the reflected beam hits the high-reflecting coated part of the front surface in such a way the beam progressively bounces between the two surfaces. At each reflection on the back surface, a new wave is formed whose position can be mapped to a vitual image at a periodic position on an axis defined by Θ_{VIPA} (refer to figure 15a). The resulting wave-front is a coherent combination of the array of virtually images, producing an angle Θ_λ at the output. Due to chromatic dispersion as the beam propagates through the bulk material, different spectral modes will propagate at slightly different angles and, thus, output at slightly different Θ_λs. Although we focus on the dependece of Θ_λ on the input wavelength, it is important to keep in mind that is also depends on the thickness t, index of refraction n, and angle with respect to normal incidence Θ_{VIPA}.

In figure 15b, the full setup for the VIPA-based SSMM is shown. In this case, the input light contains three different spectral modes that exit the VIPA at three different angles. It is interesting to note that, due to the coherent combination of arrayed-virtual images, the output beam is collimated [37]. By placing a focusing lens at the output, the different angles can be mapped onto different spots (according to the inherent Fourier transform of the lens) at the lens's focal plane and, thus, collected at individual spatial modes, either by optical fibers or by so-called pick mirrors. If many spectral modes compose the input light beam, the output will look like a $1D$ array of the demultiplexed frequencies in the focal plane.

In an etalon cavity, the free-spectral-range (FSR) is a measure of how far in frequency, from the spectral mode that is being transmitted, we can go until we find another allowed spectral mode. For the VIPA, the concept of FSR takes on a slightly different meaning: two frequencies spaced by the VIPA's FSR will fulfill the same interference conditions and output at the same spatial mode, making them spatially indistinguishable. In other words, the VIPA has a limited bandwidth within which the VIPA-based SSMM can occur without spectral mode overlapping. An intersting proposal to overcome this limitation is to use a Bragg grating at the output of the VIPA so that a 2-dimensional grid of spatial modes with extended SSMM bandwidth is produced; this, of course, comes at the expense of decreased coupling efficiency [38].

6.2 Simulations and expected results

Under the correct conditions, the VIPA can be used as a suitable SSMM. Figure 16 shows a simulation of the expected SSMM light at the output when the input consists of a distinct 9-spectral-mode comb-like flat-top spectrum spanning over $54GHz$ centered at $\lambda_0 = 1550nm$. The physical parameters of the VIPA are chosen such that the FSR is $60GHz$. They correspond to the ones used throughout the experimental part of the work. The equation that governs the VIPA-based SSMM is as follows:

$$I_{out}(x_F, \lambda) \propto \exp\Big(-2\frac{f_c^2 x_F^2}{f^2 W^2}\Big) \cdot \frac{1}{(1-Rr)^2 + 4(Rr)\sin^2\Big(\frac{k\Delta}{2}\Big)}, \tag{20}$$

where the first term describes the spectral/spatial envelope and the second the interference conditions, which satisfy

$$k\Delta = k\Big[2t\cos(\theta_i) - \frac{2t\sin(\theta_i)x_F}{F} - \frac{t\cos(\theta_i)x_F^2}{F^2}\Big] = 2m\pi. \tag{21}$$

Where, $f_c = 150mm$ and $F = 1000mm$ are the input (cylindrical) and output (focusing) lenses' focal distance, $W = 2.1mm$ is the waist size of the initial collimated beam, $r = 0.95$ and $R = 1$ are the low and

high reflectivities of the back and front surfaces, respectively, θ_i is the angle of incidence and x_F is the horizontal position at the focal plane. Whilst the master equation 20 gives the intensity and position of the peaks depending on the frequency, equation 21 gives only the interference condition from which we can derive many parameters like the FSR or the output linewidth.

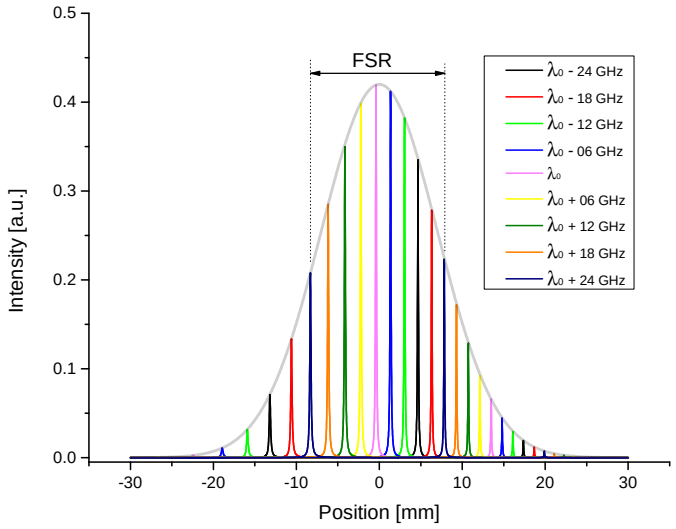

Figure 16: VIPA output simulation of a comb-like input spectra spanning $54GHz$. The same spectral mode is highlighted showing the FSR with highest power density.

A few important observations can be made based on the results of figure 16. It is clear that the VIPA configuration is optimized to transmit a given spectral mode centered at λ_0 and that the transmission of modes farther from this value decreases according to equation 20; even though the FSR can be increased to minimize the relative transmission loss as the detunings of the spectral modes increases. However, this comes at the expense of overall reduced transmissivity. In order words, transmissivity can be engineered to be more homogeneous across a broader spectral region by sacrificing its absolute value. This compromise is associated with the fact that a single spectral mode is mapped to different spatial modes: as can be seen in figure 16, all the colors appear more than once in the span of the envelope. As the envelope becomes broader, that ratio of multi-spectral mode mapping increases. Note that for the parameters of the input light for which the VIPA's FSR was matched, there is no overlap of spectral modes in the same spatial mode. That is the reason behind highlighting the FSR region in figure 16: if another spectral mode, with the same spacing, would be added, it would coincide with a spatial mode already occupied. The simulation considering the current physical parameters allows an estimated SSMM of up to 9 spectral modes spaced by $6GHz$ with a spectral resolution of $\approx 700MHz$ and a Signal-to-noise Ratio (SNR) – dominated by the cross-talk between spectral modes – of about $18dB$.

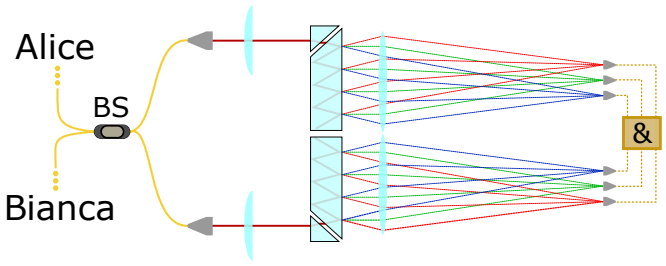

Figure 17: Configuration for frequency-multiplexed BSM and posterior demultiplexing using VIPAs as SSMMs. Detection signals of individual spectral modes are correlated after demultiplexing.

In possession of the SSMM described above, the frequency-multiplexed BSM (FM-BSM) can be as-

sembled. The setup depicted in figure 17 showcases the arrangement of beam-splitter, VIPA-based SSMMs, and a logic unit. It is important to stress that logic operations between detections stemming from detectors associated with different spectral modes, are not expected to yield BSM results. This is due to the fact that photons occupying distinct spectral modes are distinguishable and, therefore, do not exhibit HOM interference for the derivation, which is a requirement for the linear-optics-based BSM. However, the VIPA-based SSMM is not ideal and some level of cross-talk between spectral modes is expected, as will be discussed in the Results section.

It is time to put things into practice and implement experimentally the main object of the thesis: a FM-BSM. In the following sections a detailed explanation of the experimental apparatus and their characterization is provided. Finally, the obtained figures of merit are showed and discussed.

7 Experimental Setup

Between the three main steps towards a repeater chain that we have discussed, QKD, teleportation and entanglement swappings; the MDI-QKD is the simplest form that showcases a BSM. For that reason, we have put together a setup that replicates an MDI-QKD experiment. Moreover, the experimental setup, depicted in figure 18, is multiplexed in frequency like the one in frequency-multiplexed quantum repeater architecture. As the reader will come to learn, the design of this experimental setup was made such that an upgrading towards quantum teleportation is possible by just replacing a few fibers and adjusting parameters from our control-unit. We use the setup to characterize different pieces of technology, that will be employed in building a quantum repeater and that were partly developed during the thesis. Mainly, interferometer-stabilization and frequency-multiplexed BSM.

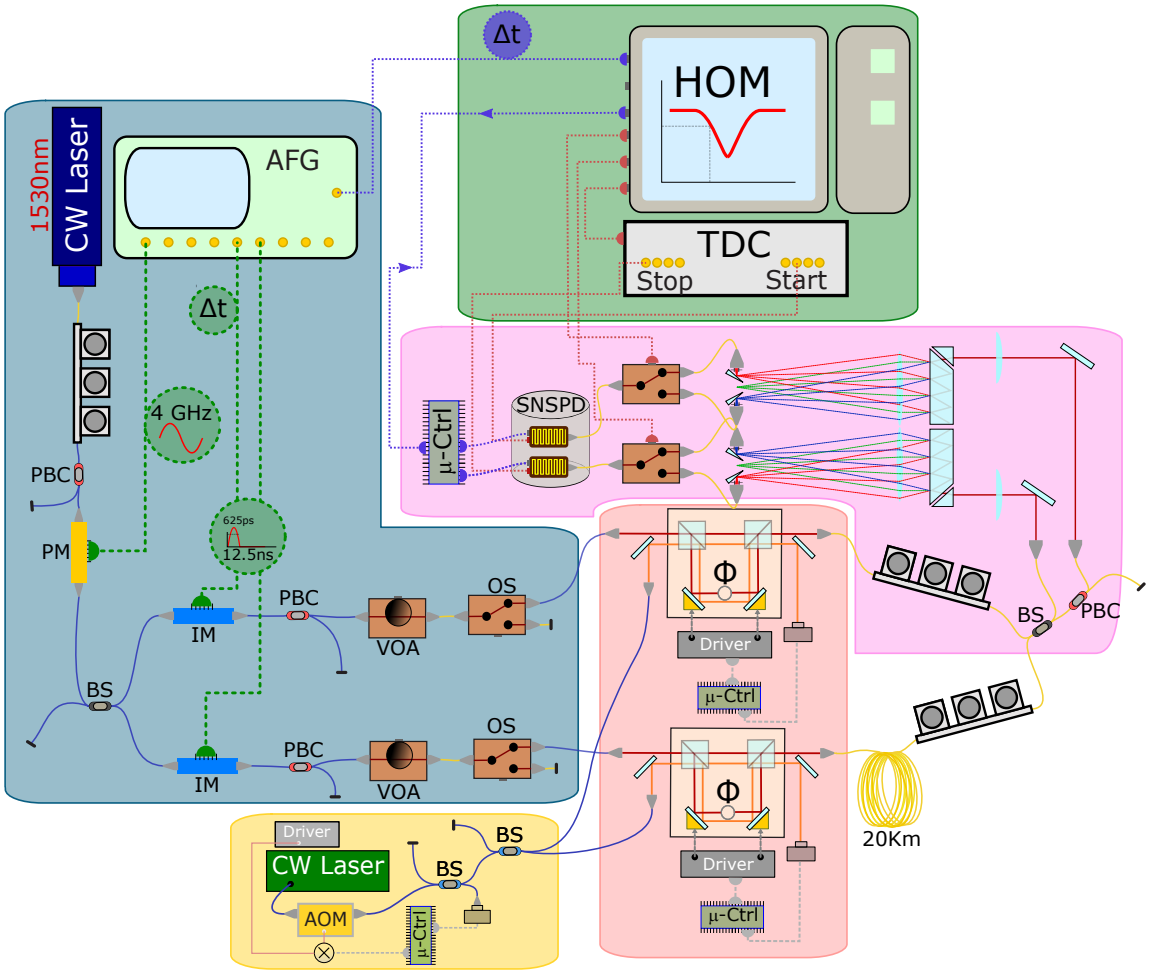

Figure 18: Experimental setup.

In the picture, we can distinguish differently colored areas. Each one has a specific purpose:

- **Host preparation** (*Blue*): This part is in charge of generating and shaping the light that will be distributed through the entire system. It starts with a laser and, at the end, we have two fibers, each one containing pulsed light at the single-photon level. Moreover, these pulses are frequency-multiplexed, mimicking a simpler version of the emission from the EPPS, as only two spectral modes are considered. One could think of this setup as an MDI-QKD setup in which Charlie also distributes the light to Alice and Bianca to ensure they have the same spectral distribution and the correct timing.
- **Intensity stabilization** (*Yellow*): For reasons that will become clear later, Alice and Bianca also share a different laser than the one for communication. It will be used for stabilization of the interferometers. This part ensures that the output power of the stabilization laser is constant and is distributed to Bianca and Alice.
- **Qubit encoding** (*Salmon*): Here, having received the light form Charlie, Alice and Bianca encode their qubits using their respective interferometers. The setup for controlling their phases and stabilization is also depicted.
- **Frequency-multiplexed BSM** (*Pink*): After the interferometers, the qubits travel towards Charlie. Bianca is $20km$ of spooled fiber away from Charlie, whereas Alice is quite close by. The polarization can be adjusted by Charlie right before the interference of the qubits in the BS. After interference, Charlie demultiplexes the frequencies to distinguish which ones were successful and the states they were projected on. In this part, the VIPAs are used and the spectral modes coming from either output of the BS are collected individually and detected. Since this part is related to the final results of the thesis, it will be thoroughly discussed in the Results section.
- **Control and measurement** (*Green*): This part is in charge of collecting and processing data as well as controlling the entire experiment and its parameters.

7.1 Host preparation

We start with the continuous-wave laser, or carrier, as the main source of light that will be shaped and distributed. The laser, with its output already fiber coupled, emits at $1532.68nm(\lambda_0)$ with an output power $\approx 4.5mW$. It is sent through a polarization beam-combiner (PBC) to ensure one pure polarization state, which is important as our devices' efficiency depends on the input polarization mode. A phase-modulator (PM), driven by a $4GHz$ sinusoidal electrical signal, creates multiple side bands [39]. Effectively, we are only interested in the first side bands as they have the most power and an equal power distribution. The laser is modulated in frequency such that $\nu_{\pm} = \nu_0 \pm 4GHz$. In the end, we have two spectral modes separated by $8GHz$ and a central mode (the carrier) that will be suppressed, as it is not relevant.

The output of the PM is split equally and sent to two identical arms; as explained before, either arm represents Alice and Bianca. Sharing the same source of light for their qubits facilitates the experimental procedures as no laser-locking for frequency stabilization is needed. If Alice and Bianca send their qubits encoded into the same spectral modes, one of the conditions for two-photon interference is instantaneously met. First, the continuous laser light is sent through an intensity modulator (IM) that acts as a shutter, pulsing the light. The IMs are pulsed periodically with squared electrical signals of $625ps$ of duration and $80MHz$ repetition rate. To ensure perfect time overlap of the pulses on Charlie's beam-splitter, one of the IMs is driven by an electrical pulse that can be delayed with respect to the other. Although higher frequencies could have been used, the $80MHz$ rate is chosen to match that

of an SPDC-source that is present in the same lab. The reason behind this is to use part of the experimental setup to perform frequency-multiplexed quantum teleportation in the near future. Secondly, the pulses are attenuated by a set of remote controlled variable optical attenuators (VOA). That will bring our pulses to the single photon level, and by adjusting the bias voltage on the attenuators one can adjust the mean photon number μ contained in each pulse. This is an important practical aspect of the decoy state method implementation.

The characterization of the attenuation and loss in the optical setup, combined with the detection efficiency is summarized in figure 19. As will be demonstrated later in section 8.1, when dealing with non-ideal single photon sources (a coherent source, in our case) one has to ensure the same mean number of photons in each input-arm of the BS in order to maximize the efficiency of the linear-optics BSM.

Finally, an optical switch (OS) is placed for mere testing purposes: it allows us to turn on and off each one of the arms individually without the need to break the connections in the setup. This is used for characterization and control of the IMs, attenuators and polarization, as well as characterization of the temporal shape of the pulses in each arm individually.

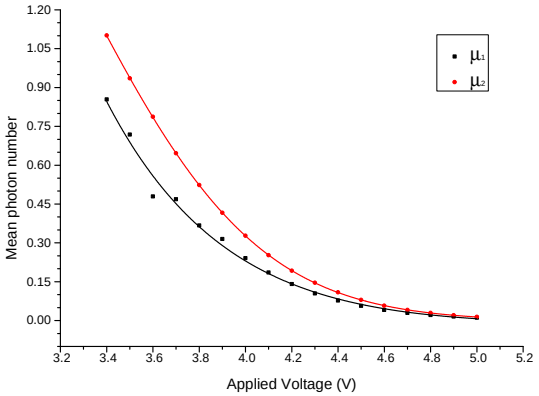

Figure 19: Mean number of photons in each arm reaching the beam-splitter versus the applied voltage to the VOAs.

7.2 Qubit encoding and interferometer stabilization

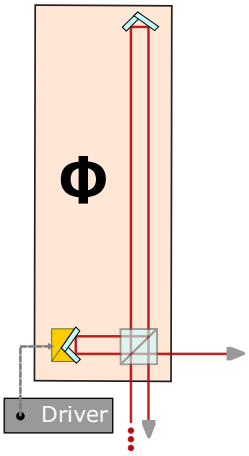

Figure 20: Mach-Zender interferometer with a movable mirror mounted on a piezo-stage that allows controlling over the phase Φ by adjusting the path-length difference.

In section 2.2, we explained how, by means of a Mach-Zender interferometer, we could can any qubit state. In this section we report the physical implementation of such interferometer, including the necessary phase stabilization.

Following picture 20, the employed interferometers are folded, free-space-based Mach-Zender interferometers with large path-langth difference. Pulses of light or photons enter the interferometer and splits, into different arms; retro reflectors are situated in such a configuration that the photons are sent back to the initial BS along a slightly different optical path. Because of the path length difference the optical pulses arrive at different times defining the two temporal modes of a time-bin qubit. Careful optical alignment ensures that early and late time-bins are collected in the same spatial mode. Note that figure 18 does not depict folded interferometers simply for readability of the drawing.

As previously discussed, the element that allows controlling the phase between early and late time-bins is the length difference between the arms. Hence, to stabilize the phase of the photonic qubits, it is mandatory that all changes in environment that can affect the relative path are taken care of and countered, i.e. controlled

As a first step, the interferometers are enclosed in a thermally controlled box, regulated with a resistive element that maintains a constant temperature due to a feedback loop implemented with a temper-

ature sensor. This becomes much easier with a folded interferometer as the volume is smaller. However, this solves the problem only potentially. To acquire absolute stability, we also send frequency stabilized continuous wave laser light through the interferometers. To ensure minimum cross-talk, its frequency and spatial mode differs from those of the photons used for quantum communication. The measured intensity captured at the detector of the output is:

$$I \propto |E_1 + E_2|^2 = \left| e^{-i\varphi} \left(E_0 + E_0 e^{i\Phi} \right) \right|^2 = 2(E_0)^2 (1 + \sin \Phi) \tag{22}$$

where E_0 is the electric field amplitude in each arm and Φ is the acquired relative phase difference.

Using a laser with a very well defined and stable frequency (therefore, a long-coherence time), one can measure the output power and observe how it changes according to the optical path variation. To counteract the phase-drifting, one of the mirrors is replaced by a movable-mirror mounted on a piezoelectric element. By changing the voltage applied to the piezo element, the path length difference is altered, thereby the relative acquired phase, and, finally, the measured intensity. Figure 22 shows the configuration: the optical path for the stabilization (light orange) with its corresponding detector and a micro-controller that allows for automatic correction of the phase by acting on the piezo element through a driver.

Relevant aspects for phase stabilization using this technique are: highly coherent light; and intensity stability. If the latter were to change over time, the feed-forward loop would understand it as a change of the interferometer's phase. That is why we also submit the light to a loop for intensity stabilization. For this purpose, we make use of an electro-optical modulator (EOM) a beam-splitter, a detector, and a microcontroller that closes the feedback loop.

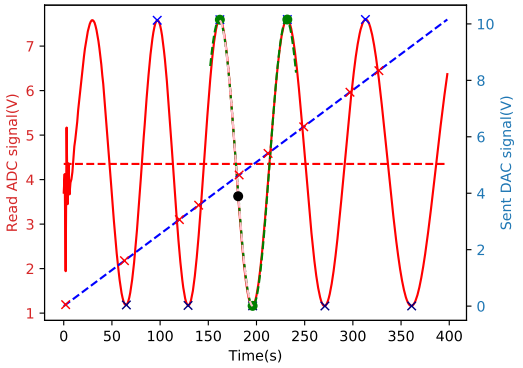

Figure 21: User selected setpoint for PID-stabilization (black dot) at $\Phi = 100deg$. In blue (dashed line), the applied voltage to the piezo-controller. In red, the corresponding transfer-function according to 24. In green, the vecinity of the setpoint. (Horizontal axis in arbitrary units instead of seconds).

7.2.1 Interferometer stabilization

Three main components are used for the stabilization of the interferometers we employ. These are a piezo-element that acts on the phase; a detector that allow us to probe the phase; and a micro-controller that, based on the detector's reading, controls the applied voltage to the piezo.

The micro-controller board consists of an Arduino (programable processing unit with a small flash memory) board equipped with an analogic-to-digital converter (ADC) and a digital-to-analog converter (DAC). The micro-controller, although programmed to work as a stand-alone unit, is constantly communicating with a personal computer so that the user can periodically check the status of the system.

The main function of the micro-controller is implementing what is known as a proportional-integral-derivative controller, or PID, for short. A PID is a control loop that produces a correction signals based on the calculation of an error value. The latter is determined as the difference between a so-called "set point" and the current value of a given observable variable of the system. The former can then be used to act on the system so that the error signal is minimized. PID's are present in a lot of environments in our daily life. A very familiar application of a PID system is the cruise control of a car: a desired velocity is fixed and, to maintain the velocity stable, the engine will automatically regulate the acceleration accordingly to dynamic environmental changes.

The correction needed for the system $u(t)$ from equation 23 takes into account how far the system is from the stabilization point in terms of the current (proportional term), the past states (integral term) and the immediate change of the observable (derivative term). All these contributions are weighted by the coefficients K_p, K_i, K_d which need to be adjusted based on the properties of each individual system.

$$u(t) = K_p e(t) + K_i \int_0^t e(t')dt' + K_d \frac{d}{dt} e(t) \tag{23}$$

PID's are usually used in a feed-forward configuration, very much like the one we have depicted: there is a system (the interferometer), whose phase we want to control. The observable, however, is the intensity measured at its output, which of course, has a direct (a priory known) relationship with the phase. How to determine this relationship is an important part of the stabilization. When the weights (K_p, K_i, K_d) are correctly tuned, the correction signal will act to stabilize the signal over time such that the mean is equal to the set point and the standard deviation is minimal.

In order to implement the control routine in a micro-controller, it is necessary to resort to the discrete time version of the PID control loop, where integrals become summations and derivatives become first-differences. Provided that the sampling rate of the ADCs and DACs meets the Nyquist criterion of the system's time evolution transfer function, convergence will be achieved. The following is a simple schematics of the protocol that the PID runs inside the micro-controller for phase stabilization:

0. The phase is stable at Φ_0, corresponding to a fixed measured output power P_0 and mirror position x_0.
1. A phase altering phenomena happens and the optical power measured at the detector increases (decreases) to P_1.
2. The corresponding electrical signal is fed into the micro-controller which, based on the current and previous states of the system, computes de correction needed in a given iteration.
3. A signal is sent from the micro-controller to the driver that acts on the piezo so that the mirror is displaced to a new position x_1, with a micro metric precision.
4. Go to 1.

7.2.2 Stabilization over time

The interferometer phase stabilization offers an extra degree of complexity due to: (i) the non-linear relationship between the applied and measured signals (as of equation 24); and, (ii) the fact that the piezos have a maximum displacement range. The effect of (i) and (ii) is that, as time goes on, the system evolves to maintain the error signal at a minimum value but with no guarantee that the actual phase of the interferometer is the required one. Consider the transfer function of the system, hereby defined as

$$\frac{V_{out}}{V_{in}} = I_0 \cdot \cos(\Delta\Phi) \tag{24}$$

It can be readily seen that, for multiple values of the relative path phase difference $\Delta\Phi$, the function assumes the same value, which is the effect of (i). Consider in addition that the environmental changes over time direct the output to its absolute maximum value, corresponding to a maximum displacement of the piezeo element. Further changes will not be correctly compensated by the system because the piezo simply has no room left to move. Given that both these effects would compromise the reliability of the phase and, in turn, of any measurement that depends on it, a routine was developed to periodically confirm the stability of the phase value. During the initial step of the stabilization procedure, as already mentioned, the piezo's displacement is swept and the corresponding intensity values are measured and

stored; this allows the user to select any given set point of the phase based on the value of the intensity. It also provides a reference measurement of what the vicinities of any given point in the transfer function should look like. The check routine is simply a comparision of said vicinity (as the time evolves and also the PID) with the very first reference measurement. In practice, it is implemented periodically at every 25 seconds, i.e, the system, with the PID, evolves freely for 25 seconds and, then, a quick sweep around the current value is performed (200ms long) so that the region around the current set point is determined. The system then compares this measurement with the first one and either resumes the PID routine in case the curves are similar (in a least-squares error sense) or warns the user that the system needs to be recalibrated. In order to showcase the stability achieved with our solution over time, we present, in figure 22, the superposition of more than 4000 curves measured with the check routine over a period of 36 hours.

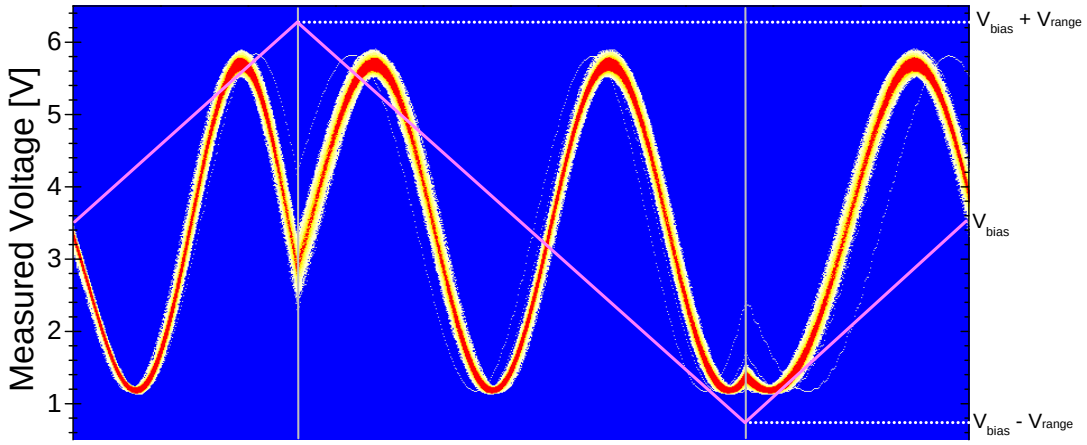

Figure 22: Time-evolution of the vecinity of the stabilized Setpoint. The heatmap is obtained by superposing more than 4000 measurements taken over a period of 36 hours.

This result proves that we have been able to guarantee phase stability over times long enough so that experiments can run reliably. Probing of the state of the PID during the self-check routine disturbs the system for a small time but does not prevent it to recover the same stabilization point, providing a robust way to monitor its evolution. Times as short as $1ms$ are enough to stabilize the system.

The intensity control loop for the probing laser operates in a similar way, but without the need of a check routine since the measured value already corresponds to the information of interest (the intensity).

7.3 Spectral-to-Spatial Mode-Mapping: characterization

Following figure 18, the frequency-multiplexed states prepared by both Alice and Bianca are sent to both inputs of a symmetric beam-splitter. At the output, after going through a polarization beam-splitter for polarization stabilization (discussed in the next section), the output beams are cast into free-space and input into the VIPA-based SSMM setup. The spectral modes of interest are those corresponding to the sidebands at $\pm 4GHz$, as created by the PM; thus, at the focal plane of the focusing lens, a so-called offset mirror is placed such that the center spectral mode (the original optical carrier) is spatially filtered by a narrow gap. The shifted spectral modes are displaced such that they bounce off of the mirrors and can be efficiently coupled into individual fibers. We estimate a 5-10% system efficiency i.e., fiber-to-fiber coupling efficiency of the different spectral modes through the VIPA. We assume that the losses are due

to spatial mode mismatch at the input of the single-mode collection fibers since the ellipticity induced by the cylindrical lens might not be perfectly compensated by the VIPA. At the input of the collection fiber, it is possible to measure a $\sim$ 60% transmission through the VIPA using a free-space power-meter.

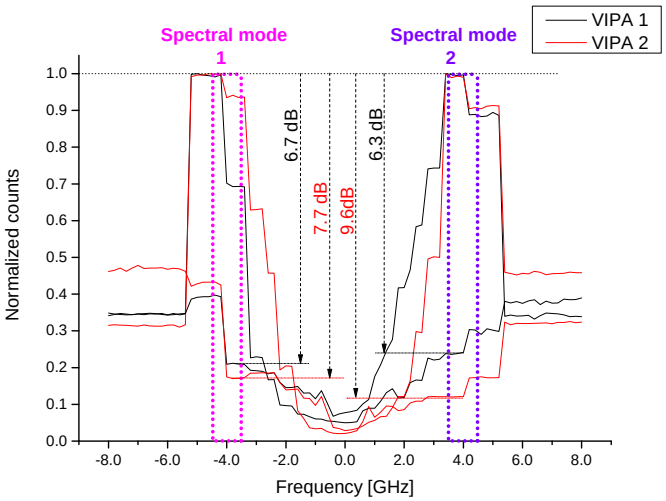

Figure 23: VIPA demultiplexing characterization.

One important characteristic of the demultiplexing is the signal-to-noise ratio (SNR), with cross-talk of adjacent spectral modes being its main component. Figure 23 reports normalized single-photon counts detected by detectors matched to the spatial modes associated (through the VIPA-based SSMM) to the $\pm 4GHz$ spectral modes generated up to a first order approximation by the PM. The figure is obtained scanning by frequency-shifting the optical carrier in a $\pm 8GHz$ range using serrodyne modulation, effectively shifting the optical carrier to a specific spectral mode as opposed to creating multiple sidebands. Using this technique, we can scan the frequency of the shifting across a broad spectrum and spectrally characterize the VIPA-based SSMM, thus allowing us to compute the cross-talk at each spatial mode.

The two spectral windows emphasized in figure23 correspond to the modes of interest ($\pm 4GHz$). To estimate the cross-talk at spectral mode 1 of VIPA 1, one can sum the contributions from the carrier and spectral mode 2 of VIPA 1, obtaining $6.3dB$ SNR. The cross-talk for the other modes are obtained in a similar fashion. The significant difference between the simulated $\sim 18dB$ and the experimentally measured results is remarkable. Once again, we associate these differences to the spatial mode-mismatch and the rather static configuration of the offset mirrors, that, although able to suppress the central mode, does not allow for perfect filtering the sidebands. Despite the discrepancy, the estimated cross-talk values are in a range that allows for a clear distinction between spectral modes.

In the real-case scenario, one would have one single-photon detector at the end of each spatial mode. However, due to current resource limitation in the laboratory, only two such detectors are available. In order to enable automated measurement of all the possible combinations of spectral modes, the outputs of the SSMM were directed to two optical switches (refer to figure 18) that can be remotely controlled. Although the current method prevents us from achieving the higher throughput enabled by the frequency-multiplexing, it allows for full system characterization; the successful BSM rate that would be achieved with active multiplexing is the sum of the rates of each spectral mode.

In figure (24), the time-referenced normalized counts measured using a time-to-digital converter after the VIPA-based SSMMs are depicted for different qubits: $|\ell\rangle$ and $|+\rangle$. The detectors employed are Superconducting-Nanowire Single-Photon Detectors (SNSPD) working inside a cryostat at $0.83K$, reporting a $sim60\%$ detection efficiency with $300Hz$

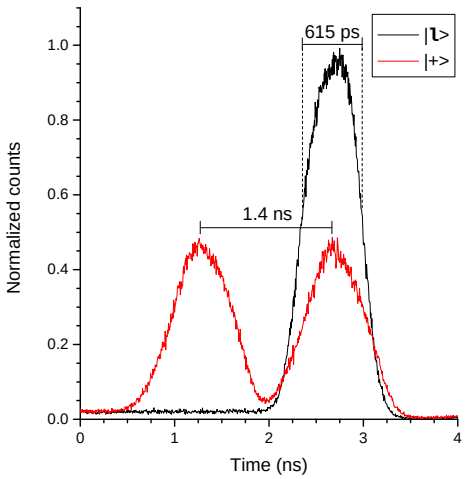

Figure 24: Temporal mode profile for qubit states measured after demultiplexing.

dark-count rate. We can see that they exhibit a full-width at half maximum (FWHM) of roughly $615ns$; this is expected, since the electrical pulses used to generate the optical pulses exhibit a temporal duration of $625ns$. Also, the design of our interferometers creates a late time-bin with a $1.4ns$ delay with respect to the early bin. One factor that affects the purity of our states is the little cross-talk between the temporal bins of the $|+\rangle$ state, partly due to response capabilities of the detector. As indicated in a previous section, μ was adjusted to be the same when generating Z- and X- basis qubits.

7.4 Control and measurement

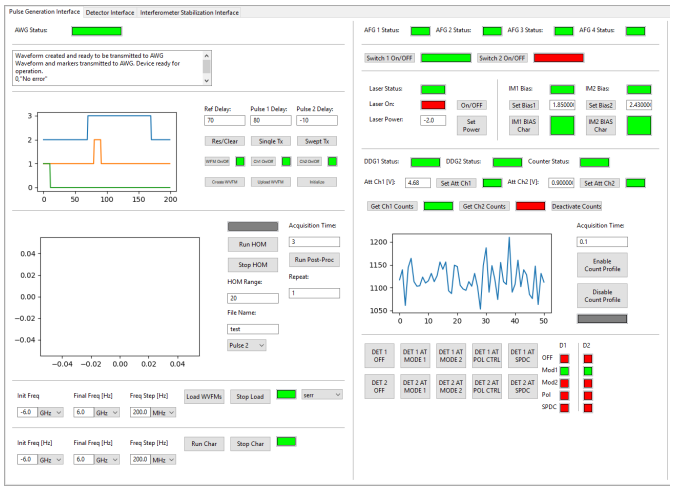

Figure 25: Main tab of user interface to control and automate sub-routines. The second and third tabs (not shown) are for SNSPD control and interferometer stabilization (figure 21 is extracted from this tab).

The last major unit that composes the experimental setup is a computer program (doted with an user-friendly interface, figure 25) that enables the control and automation of all aspects of the experiment. A variety of functionalities is implemented by the control program, including, but not limited to: the VIPA-based SSMM characterization presented in figure 23; electric pulse generation control – that, in turn, controls the arrival time of optical pulses at the remote BSM –; automatic adjustment and unlatching of the employed SNSPDs; and phase selection and phase-stability monitoring for X-basis qubit generation.

The goal of an automated control unit is being able to control and stabilize, over time, all the degrees-of-freedom of the photonic wave-packets that interact in the BS, i.e., polarization, intensity, temporal mode, spectral mode, and spatial mode. The last two do not require control: the latter because the fibers employed are single-mode fibers, thereby defining the spatial mode of the wave-packets; and the former because a single laser was employed to distribute light to Alice's and Bianca's station, rendering the spectral modes identical. Polarization is controlled through a feedback system composed of the remaining output of the PBC, a single-photon detector, and a remote polarization controller. After coarse manual control, the polarization can be kept stable for days with the control unit.

Intensity, as has been previously mentioned, is controlled using an electrically-tunable optical attenuator (VOA). The control routine detects deviations in the measured counts and can compensate in the event they cross a pre-established threshold. Finally, and more importantly, by controlling the temporal modes of the wave-packets in terms of the arrival time of the optical pulses at the BSM, it is possible to extract the so-called HOM-dip, i.e., the reduction of the measured coincidence counts as the pulses become indistinguishable[5]. This important measurement is performed by controllably sweeping the delay time at small steps and recording the measured coincidences.

One fundamental limitation can already be discussed. Given the sample rate of the arbitrary waveform generator (AWG) that was used ($16GSamples/s$) one can only obtain a temporal resolution of $62.5ps$, that is 10% of the duration of the optical pulses. Given our limited temporal resolution, there might be some configurations of the delay that do not allow for the visibility to reach maximum. This effect is revealed when consecutive HOM dip measurements are performed, yielding vastly different

[5]Refer to Appendix C and section 8.1 for a discussion regarding the experimental HOM dip.

traces (different positions of the minimum and visibilities) due to changes in the 20km optical fiber coil. Subtle changes of the local temperature cause stretching of the fiber and change of the refractive index affecting the optical path. That leads to a limitation of the time during which we have to perform one of such measurements before the state of the system changes too much; as well as post-processing if one is averaging over measurements.

8 Results

The experimental setup described in the previous section implements a simplified MDI-QKD link, with Alice and Bianca sharing the light source used to prepare their photonic qubits. The point of this experiment, as previously stated, is to provide a robust framework for testing the demultiplexing capabilities of the proposed VIPA-based spectrally-multiplexed LO-BSM solution. Although the actual BSM information (the projection on one of the four Bell states) is the ultimate goal of the experiment, the characterization of the HOM effect, the core of the LO-BSM[6], provides a rich tool to investigate the characteristics of our system. Based on the parameters extracted from the so-called HOM-dip visibility, it is possible to estimate, through a robust simulation tool, the secret-key rates achievable for each employed spectral mode and, thus, an overall improvement factor of the spectraly-multiplexed versus regular LO-BSM in an MDI-QKD scenario.

8.1 Frequency-multiplexed HOM

The Hong-Ou-Mandel effect is a two-photon interference phenomenon that takes place in a symmetric beamsplitter fed by two indistinguishable photonic wave-packets. Its basic physical underlying principle is the destructive interference of the joint wave-packet that describes the two input states taking opposite spatial modes at the output. The phenomenon is characterized by a reduction of the coincidence detection rate between two photodetectors placed at the output of the beamsplitter. Because the destructive interference is associated to the joint wave-packet, it only materializes when the two input states are indistinguishable, becoming a useful asset for measuring the degree of distinguishability between photonic wave-packets [40]. Experimentally, we are interested in the so-called HOM dip visibility, i.e., the contrast in coincidence detection rates between the distinguishable and indistinguishable cases. Therefore, in order to experimentally acquire a HOM dip, one must have full control of all degrees-of-freedom of the interfering wave-packets – intensity, temporal mode, spectral mode, polarization mode, and spatial mode – so that, not only can they be made indistinguishable, but also controllably distinguishable.

With ideal single-photons, the HOM visibility can reach 100%; it decreases in case the photon-number distribution deviates from the ideal case. In the presented experimental setup, Alice and Bianca utilize weak coherent states for their MDI-QKD section, which corresponds to a photon-number distribution even farther away from ideal than of those states generated in an SPDC source[7].

Let us consider the input weak coherent states received by Charlie in the remote station. For simplicity, let us also consider that the states occupy a single spectral mode, instead of multiple ones, and that all other degrees-of-freedom are indistinguishable except for the parameter of the coherent state. Under these conditions, the joint input state can be written as

$$|\Psi_{\text{in}}\rangle = |\alpha\rangle_{a_{in}} \otimes |\beta\rangle_{b_{in}} = \hat{D}\left(\alpha\right)_{a_{in}} \otimes \hat{D}\left(\beta\right)_{b_{in}} |0\rangle_{a_{in}} |0\rangle_{a_{in}} \tag{25}$$

where $\hat{D}(\alpha)$ is the displacement operator[8]. The coherent state parameters α and β are complex, and contain phases that have to be taken into account. Because care is taken in the experimental realization to make sure that the interfering photonic qubits are outside of each other's coherence region, these phases are random and, thus, the input state's density matrix can be written as:

$$\rho_{\text{in}} = \int_0^{2\pi} \frac{d\theta_\alpha}{2\pi} \int_0^{2\pi} \frac{d\theta_\beta}{2\pi} |\Psi_{\text{in}}\rangle \langle\Psi_{\text{in}}| \tag{26}$$

[6]The reader is referred to Appendix C for a more in-depth discussion.
[7]see Appendix A
[8]same notation from the appendices is used for this derivation

After the BS transformation[9], the structure of the displacement operators allows one to write the output state as:

$$|\Psi_{\text{out}}\rangle = e^{-\frac{\mu_a+\mu_b}{2}} e^{\alpha\left(\sqrt{\eta}a^\dagger+\sqrt{1-\eta}b^\dagger\right)} e^{\beta\left(\sqrt{1-\eta}a^\dagger-\sqrt{\eta}b^\dagger\right)} \tag{27}$$

One can find the probability of obtaining m (n) photons at the output port a (b) to be

$$P_{m,n}^{(out)} = e^{-\mu'_a-\mu'_b}\frac{(\mu'_a)^m(\mu'_b)^n}{m!n!} \tag{28}$$

where

$$\mu'_a = \mu_a\eta + \mu_b(1-\eta) + 2|\alpha\beta|\sqrt{\eta}\sqrt{1-\eta}\cos\left(\theta_\alpha-\theta_\beta+\theta_0\right)$$
$$\mu'_b = \mu_a(1-\eta) + \mu_b\eta - 2|\alpha\beta|\sqrt{\eta}\sqrt{1-\eta}\cos\left(\theta_\alpha-\theta_\beta+\theta_0\right)$$

The probability of having a coincidence i.e. at least a photon in each output, can be then obtained from equation 28 as

$$P^{(coinc)} = \left(1-e^{-\mu'_a}\right)\left(1-e^{-\mu'_b}\right), \tag{29}$$

which after integrating for phase-randomization like in equation 26 one can obtain

$$P^{(coinc)} = 1 - e^{-(\mu_a\eta+\mu_b(1-\eta))}I_0\left(2\sqrt{\mu_a\mu_b}\sqrt{\eta}\sqrt{1-\eta}\right) - e^{-(\mu_a(1-\eta)+\mu_b\eta)}I_0\left(2\sqrt{\mu_a\mu_b}\sqrt{\eta}\sqrt{1-\eta}\right) \tag{30}$$

Moreover, the individual probabilities of having at least a photon in each arm regardless the state of the other are

$$P^{(a)} = 1 - e^{-(\mu_a\eta+\mu_b(1-\eta))}I_0\left(2\sqrt{\mu_a\mu_b}\sqrt{\eta}\sqrt{1-\eta}\right) \tag{31}$$

$$P^{(b)} = 1 - e^{-(\mu_a(1-\eta)+\mu_b\eta)}I_0\left(2\sqrt{\mu_a\mu_b}\sqrt{\eta}\sqrt{1-\eta}\right) \tag{32}$$

where I_0 is the zero-order modified Bessel function.

The HOM-dip visibility can be calculated using

$$V_{HOM} = \frac{P^{(a)}P^{(b)} - P^{(coinc)}}{P^{(a)}P^{(b)}} \tag{33}$$

and, finally, we can simplify our equations 30, 31, 32 by using a 50:50 BS ($\eta = 0.5$, this implies $P^{(a)} = P^{(b)}$) and using $\mu_a = \mu$, $\mu_b = \lambda\mu$ where$\lambda \in [0,1]$, to obtain:

$$V_{HOM} = 1 - \frac{1-2e^{-\frac{\mu(1+\lambda)}{2}}I_0\left(\mu\sqrt{\lambda}\right)}{\left(1-e^{-\frac{\mu(1+\lambda)}{2}}I_0\left(\mu\sqrt{\lambda}\right)\right)^2}. \tag{34}$$

One can demonstrate that equation 34 has maximum for $\lambda = 1$ i.e., both sources have the same mean-photon number. Moreover one can show that $0 \leq V_{HOM} \leq 0.5$, achieving 0.5 as $\mu \to 0$ [41]. The reason behind the HOM-dip visibility drop as μ increases is due to the increased likelihood of multi-photon pulses. These pulses can either yield coincidences on their own given a multi-photon pulse on one arm of the BS and a a $|0\rangle$ on the other; or, interfere and still give coincidences due to the presence of more photons on one side than the other.

[9]The reader is referred to Appendix B for an in-depth discussion.

Finally, it is noteworthy to mention that experimentally, despite being true that lower μs result on higher visibilities and therefore, higher BSM efficiencies; decreasing too much the value will increase the number of pulses containing no-photons and hampering our rate heavily. One must find a balance between both.

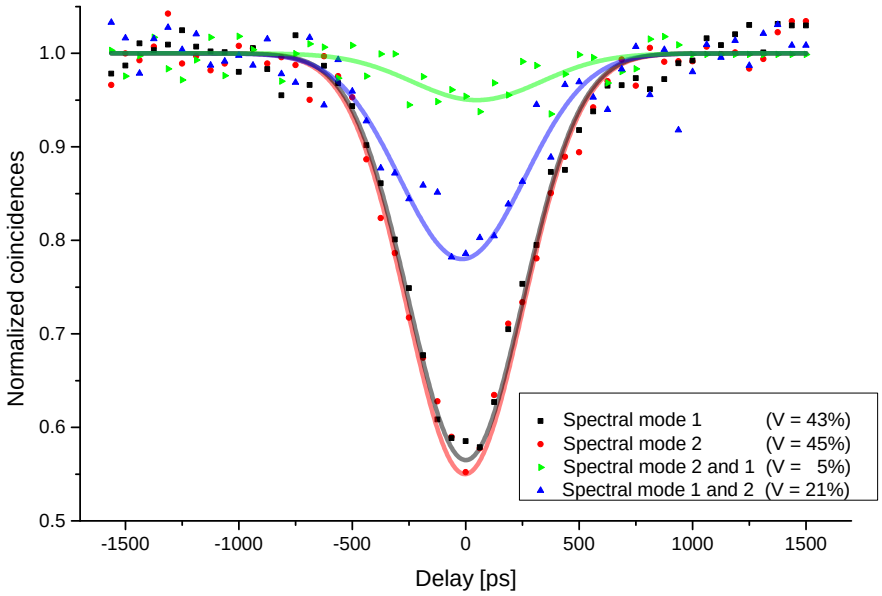

Figure 26: Frequency-multiplexed HOM dip. The four curves report the trace obtained by detecting matching and un-matching spectral-modes. The temporal degree of freedom is scanned by modifying the delay on the pulse generation.

Figure 26 reports the results of the frequency-multiplexed HOM dip between the different combinations of spectral-modes coupled after the VIPAs, allowed by acting on the optical switches for mode selection. The pulses employed are obtained by blocking one of the arms of the interferometers, in this case $|e\rangle$.

The obtained results for matching spectral modes imply that the experimental setup grants enough control over all relevant parameters, as the reported values are close to the limit for $\mu \approx 0.09$ of $\sim 48\%$ [41]. On the other hand, the curves obtained from non-matching spectral modes suggest that the optical alignment of the demultiplexing could be optimized. Moreover, having a HOM-dip trace with non-correlated spectral modes, while achieving a high visibility with the correlated ones, suggests that the imperfections in the optical alignment result in coupling loss but not necessarily in a worse BSM. In other words, the gain is reduced whilst keeping a similar QBER.

Despite having a certain degree of indistinguishability in non-matching spectral modes, when performing an MDI-QKD protocol one would only look at channels that are correlated, because no relevant information can be obtained from the crossed ones. A more discussion is procured in section 8.3.

Lastly, we obtain an average FWHM of the dips $627ps$ a value that is in excellent agreement with the expected pulse width of $625ps$ and the measured temporal profile of $615ps$.

8.2 Qubit interference curves

Once a good, consistent and reproducible degree of indistinguishability has been obtained, we can use both arms of the interferometers to create qubits at the equator of the Bloch sphere. As explained, μ needs to be adjusted given that now our pulses are doubled in energy so that we recover the same $\mu \approx 0.09$.

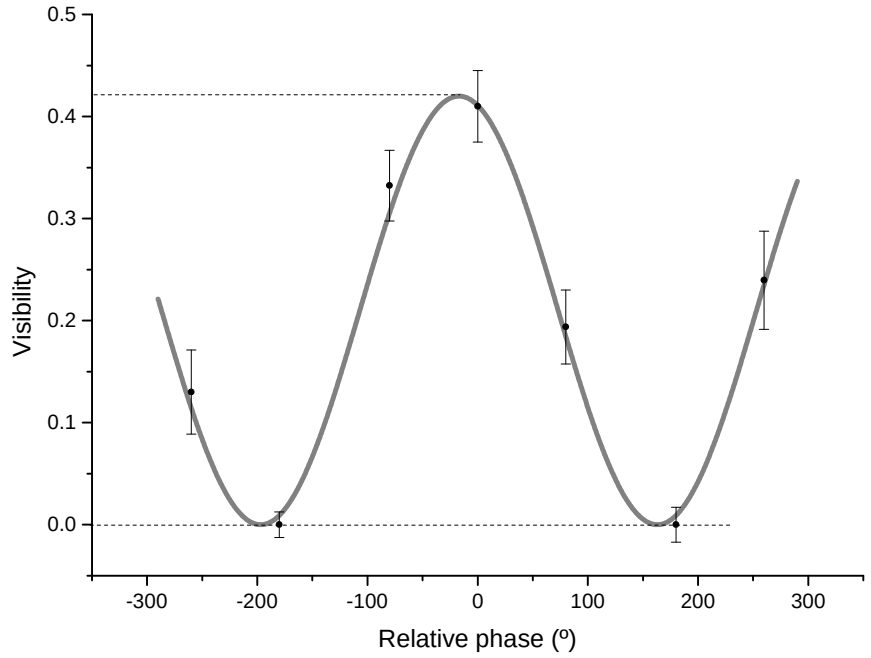

Figure 27: Qubit visibility curve obtained performing a HOM-like experiment while varying the relative phase of the qubits.

Figure 27 reports the results of a HOM-like experiment using superposed states and collecting only spectral mode 2 (maximum visibilty obtained is 45%). Each point represents an average of 10 HOM experiments following the same procedure than in the previous section. To obtain the curve one varies the relative phase between Alice's and Bianca's interferometers so that $V \propto V_{max} \cos(\phi_A - \phi_B)$.

We report in this experiment $V_{max} = 42\%$, confirming that the efforts for phase selection and the time-stabilization work as expected since we obtained almost the same results on our HOM-like experiments.

8.3 Secret key rate simulation

Based on [42, 43] we have performed a very thorough simulation of secret key rate in our MDI-QKD experiment that takes into account all physical parameters of the qubits and quantum channel. The simulation takes into account the SNR of the qubits, the reported HOM-dip visibility, and we have also supposed that Bianca and Alice are both communicating with Charlie using a quantum channel that has $6.5dB$ of attenuation. The qubit model uses

$$|\varphi\rangle = \frac{1}{\sqrt{1+2b}}\left(\sqrt{m+b}\,|e\rangle + e^{ie\phi}\sqrt{1-m+b}\,|l\rangle\right)$$

$$m = \frac{S_e}{S_e+S_l} \quad ; \quad b = \frac{B}{S_e+S_l} \tag{35}$$

and takes into account background noise, dark counts and cross-talk as well as the fidelity of X- and Z- basis qubits. Some of this parametrization can be seen in figure 35. With the reported values and characterizations from our experimental setup, the simulation yields the following secret key generation rates

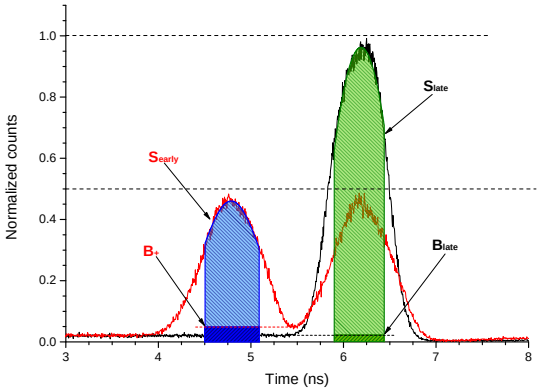

Figure 28: Qubit parametrization following equation 35. In red, the temporal profile of $|+\rangle$ and in black $|\ell\rangle$. S and B for each time-bin and state can be extracted from the noise level and the height with respect the ideal value.

	Mode 1	Mode 2
Mode 1	$4.5kHz$	$0Hz$
Mode 2	$0Hz$	$6.0kHz$

Table 2: Simulated key generation rates

We have stated previously in this work that looking at non-correlated spectral modes does not provide any relevant information for a possible eavesdropper, even if they would yield successful results on a BSM. We based this statement in the assumption that, in the MDI-QKD protocol, Charlie is a non-trusted party. Moreover, she plays a key role in the protocol by performing the BSM and forwarding the results: Charlie has all the information there is to know about the BSM and it is up to her to decide what correlations (and information) she looks at, once the photons have been detected. As we can see from table 2, if Charlie tries to implement the protocol using a combination of non-matching spectral modes, she will be effectively implementing a denial of service attack as the QBER is too high to yield any key. On the other hand, if she wishes to provide service and, at the same time, keeping the correlations of non-matching spectral modes to herself, Alice and Bianca will generate keys at the rate of $10.5kHz$, but Charlie will not be gaining information about the basis used or the generated key. Also, since Bianca and Alice implement a decoy-state protocol, any attempt to perform an attack by Charlie will be detected.

However, we acknowledge that: (i) our experimental setup encodes (at each round) the exact same qubit on the different spectral modes; (ii) using the same source of light for the different spectral modes adds a correlation between the decoy-states employed at each round of the protocol; (iii) our simulation is based in non-multiplexed MDI-QKD setups and the different spectral modes are treated independently (besides increased noise and decreased BSM efficiency due to the multiplexing). Although we have provided argumentation towards proving a secure protocol, Bianca and Alice, currently, cannot implement a communication protocol independent for each spectral mode and, to prove security, it is necessary to evaluate whether these constraints open a possible side-channel for attacks.

The main reason why this part was left as a simulation rather than brought to reality is related to the photon-detection apparatus. The employed SNSPDs have a recovery time of $\sim 100ns$. This prevents us from detecting two consecutive photons on the same SNSPD corresponding to $|e\rangle$ and $|\ell\rangle$. See how $|\Psi^+\rangle$'s projection pattern is based on this exact detection. Therefore, only $|\Psi^-\rangle$ can be measured by our detectors. Moreover, the detection signals from the SNSPDs were processed by Digital Delay Generators

(DDG). The ones used had a maximum response rate of $8MHz$, making it impossible to distinguish whether a detection had come from an $|e\rangle$ or $|\ell\rangle$ bin and also, limiting our key generation rate as we pulse with a rate of $80MHz$. These are the main reasons why no actual BSM was performed in this work but rather just the characterization of its efficiency using HOM and HOM-like experiments. In the following section, some insights about the new (already working) signal processing unit works, one that allows distinguishing $|\Psi^-\rangle$ and does not limit the detection rate.

We consider the main part of this work finished. This last section concludes the report and lays down the milestones that will be pursued next for the improvement and evolution of the project bringing it to the next step: experimental realization of frequency-multiplexed quantum teleportation.

9 Outlook

9.1 Demultiplexing and coupling

In figure 23 we reported a demultiplexing efficiency of $5-10\%$ with $6.3-9.6dB$ SNR. Although it allows for spectrally multiplexed BSM, the loss of light must be reduced to a minimum. In [37], an initial $-10dB$ coupling is reported which is then simulated to be improvable to $-3dB$ by correcting the eliptically-shaped beams before fiber coupling. We propose, as a follow up study using independent cylindrical lenses for the $\hat{x}$ and $\hat{y}$ directions [37].

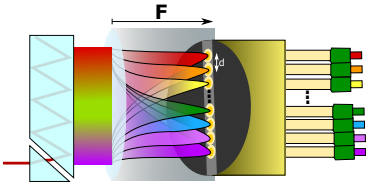

Figure 29: Fiber-bundle based demultiplexed system.

Also, the use of a lens with focal length $F = 1000mm$, although it facilitates the manual coupling now, is inconvenient for a large-scale application. We suggest moving towards a more compact demultiplexing system based on VIPA and a fiber-bundle array (as depicted in figure 29).

9.2 New detection setup for BSM detection

Even though in this work we talked a lot about BSM, no actual BSM was implemented because the limitations in the detection apparatus, as we have explained in section 8.3. The detection electronic box is already updated and now contains all the electronics necessary to detect projections onto $|\Psi^-\rangle$. The box consists of three different pieces of electronic equipment designed specifically for this task:

1. The analog signal by the breaking of cooper-pairs in the SNSPD (a detection) is sent to a comparator board. This board compares the input with a previously set bias-voltage and outputs a digital signal if $V_0 > V_{Bias}$. There is one comparator for each SNSPD.

2. The digital signal from the comparator is sent to a digitizer board. This board receives besides the signal, a master clock reference, which is used for system synchronization. Configuring the board properly with the parametrization of our qubits and the delay between the reference clock and the detection signals allows us to obtain at one of its two outputs all the detections that correspond to a $|e\rangle$ time-bin and, on the other output, the ones from $|\ell\rangle$. There is one such board for each detector.

3. Finally, the two outputs of both digitizers are sent to a Field Programmable Field Arrays (FPGA) that is programmed to compare, within the same reference clock cycle, the detections obtained. More specifically, the FPGA implements the operation $\Big(\,|e\rangle_1 \text{ AND } |\ell\rangle_2\,\Big)\text{OR}\Big(\,|\ell\rangle_1 \text{ AND } |e\rangle_2\,\Big)$, thereby indicating $|\Psi^-\rangle$ projections, although it could be also be programmed to herald $|\Psi^+\rangle$ (if the SNSPDs allowed for its detection).

The use of the comparator for digitizing the signal avoids limiting our detection rate as it happened with the DDGs. The digitizers also provide a huge improvement, not only because we can now distinguish between time-bins but because the detection window is set to match the width of the optical pulse, i.e, we disregard any unwanted detections that do not occur during the designated time-bins.

9.3 Towards teleportation

In this thesis we put together an MDI-QKD setup as this is the simplest quantum communication protocol that requires a BSM. Naturally, the next step towards entanglement swapping –a key ingredient in a quantum repeater– is quantum teleportation. Not many changes need to be made to the experimental setup, the most important being that we have to replace Bianca's setup by an SPDC source that produces a maximally entangled state, e.g. $|\Phi^+\rangle$. One photon from this source and one photon from Alice will be subjected to a BSM, resulting in teleportation of Alice photon's state onto the second photon of the entangled pair, up to a unitary transformation. Obviously, this BSM, and hence the teleportation, will also be frequency-multiplexed. While the demonstration of spectrally multiplexed quantum teleportation is similar to that of MDI-QKD, the spectral degree of freedom and the temporal shape of the pulses will need to be treated more carefully as the light proceeds from two different types of sources. In particular, the distribution of the number of photons is different: Poissonian in the case of the laser pulse, and thermal in the case of members of photon pairs. According to the Supplementary Material of [44], which presents a context equivalent to the one discussed here, the HOM visibility is limited to a value close to 30% (experimentally determined with an estimated indistinguishability of 68%). However, heralding the input from the pair source – and thereby making it approximately a single photon – changes the result, as described by the following derivation.

Let us consider for the different inputs of the BS a highly attenuated laser-pulse (a WCP $|\alpha\rangle$ with $|\alpha|^2 = \mu$) as well as a single photon. They are by all other degrees of freedom indistinguishable:

$$|\Psi_{out}\rangle = U_{BS} |\alpha\rangle_{a_{in}} |1\rangle_{b_{in}} \approx \frac{e^{-\mu/2}}{\sqrt{2}} \left[\left(a^\dagger - b^\dagger\right) + \frac{\sqrt{\mu}}{2} \left(a^{\dagger 2} - b^{\dagger 2}\right) + \frac{\mu}{2\sqrt{2}} \left(a^{\dagger 3} - b^{\dagger 3} - b^{\dagger 2} a^\dagger + a^{\dagger 2} b^\dagger\right) + \mathcal{O}(\mu^2) \right] |0\rangle_a |0\rangle_b \tag{36}$$

Assuming $\mu \ll 1$, we truncated the infinite series that describes the coherent state after the second order. We can also compute a good estimate of the theoretical maximum value of the visibility using equation 33. As opposed to the case without heralding, we find that $0 \leq V_{HOM} \leq 1$ with maximum as as $\mu \to 0$ [45].

Conclusion

We have reported an experimental setup that grants the user control over all degrees of freedom that affect indistinguishability of qubits headed for a frequency-multiplexed Bell-state measurement. This yields results such as the reported interferometer phase-stabilization, multiplexed HOM-dip visibilities and the qubit interference curve. Moreover, the simulated $10.5kHz$ key generation rate obtained by combining the contribution from both spectral modes showcases the benefits of multiplexing.

Appendices

A Photon-Statistics

Light can be characterized by many properties: wavelength, energy, spectral shape, spatial mode... In this appendix we will provide a brief experimental view on how to characterize it based on the photon statistics. To understand the concept of photon statistics let us draw a mental picture: imagine a beam of light, that can be frozen in time and of which a picture can be taken. If we were able to pinpoint the positions of the photons conforming the beam, one could try and look for correlation on how these photons are distributed in space and arranged between themselves.

Firstly, we will introduce the experimental setup that allows us to asses this property and, secondly, some insights on the theory behind it: the well-known second order auto-correlation function $g^2(\tau)$. Finally we will discuss the most relevant cases for this thesis, the coherent state of light and the single photon level.

A.1 Measuring the auto-correlation function

In figure 30 we can see the simplest experimental setup that one can use to measure $g^2(\tau)$ [46]. It is composed of a 50:50 beam-splitter, two single-photon detectors and one logic unit. The light is input into the beam-splitter and with equal probability the photons will end up at either of the output arms, where they will be detected. The logic unit will start a timer when $D1$ detects and stop it by detections at $D2$.

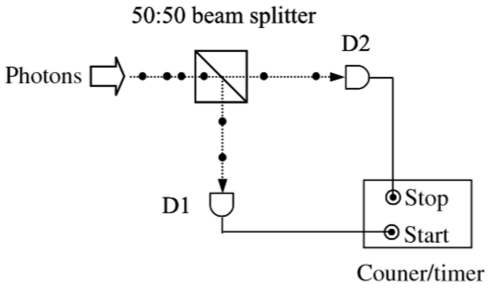

Figure 30: Experimental setup to test photon statistics. Figure borrowed form [46].

To distinguish different statistics, let us look at figure 31.

- One extreme case is if the photons arrive at the beam-splitter one by one. There will a collection of random delays between start and stop of the timer. However, since there is only a single photon it cannot start and stop the timer with $\tau = 0$ i.e., it cannot yield a coincidence detection in both detectors. The randomized delay times will provide a base-line from which a dip appears as one approaches $\tau = 0$. This case is labeled as anti-bunching in figure 31.
- The other extreme case is when the photons are organized in bunches. With small probability all of them will go to the same arm. This will result in an increase in the coincidence counts ($\tau = 0$) compared to the base-line. This case is labeled as thermal light or photon-bunching in figure 31.

The photon statistics can be discovered by the shape of the histogram at around $\tau = 0$. The figure of merit that is the histogram is well known as the $g^{(2)}(\tau)$ cross-correlation function. One can show that

$$g^{(2)}(0) = \frac{P_{1,2}}{P_1 P_2} \tag{37}$$

where $P_{1,2}$ is the probability of a coincidence measurement whereas P_1,P_2 are the individual probabilities of only one of them detecting.

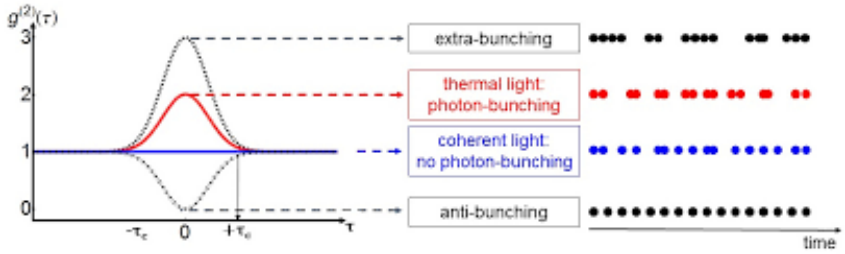

Figure 31: Sketch of light statistics with different degree of bunching and the corresponding auto-correlation histogram trace.

A.2 Second-order correlation function

The correlation or coherence functions introduced by Glauber during the 1960s [47] are used to determine the degree of coherence of an electromagnetic field. The first-order correlation function investigates correlations between the phases of fields, yielding results like the two-slit diffraction by Young[48]. In the second-order one analyses correlations between the intensities of fields, and specifically in the quantum case, between single photons.

The second-order auto-correlation function can be described by

$$g^{(2)}(0) = \frac{\langle a^\dagger a^\dagger a a \rangle}{\langle a^\dagger a \rangle^2} = 1 + \frac{\langle (a^\dagger a)^2 \rangle - \langle a^\dagger a \rangle^2 - \bar{n}}{\bar{n}^2} \tag{38}$$

where we use the variance of the number of photons

$$V(n) = \langle (a^\dagger a)^2 \rangle - \langle a^\dagger a \rangle^2 \tag{39}$$

As we experimentally discussed and depicted in figure 31, light can be classified by its degree of bunching that is mainly determined by the variance with respect to the mean number of photons. In this thesis we are mainly interested in the transition between anti-bunching and bunching. The state corresponding to the limit between the regimes is known as coherent state. It is named like for historical reasons and because its photons share a first order correlation in phase. This state is the eigenvector of the annihilation operator i.e., $a^\dagger |\alpha\rangle = \alpha |\alpha\rangle$. It can be proven that such states have a photon-statistics following a Poissonian distribution. The coherent state is described by the following superposition of number-states 40:

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_0^\infty \frac{\alpha^n}{\sqrt{n!}} |n\rangle . \tag{40}$$

Expression 40 is often written in a more compressed form by using Glauber's displacement operator $\hat{D}(\cdot)$

$$\hat{D}(\alpha) |0\rangle = |\alpha\rangle \tag{41}$$

These states, although uncommon in nature, can be engineered: a laser is a coherent source of light given that the emission is started be a single spontaneously-emitted photon that stimulates emission of other atoms in the medium. We can compute the average number of photons and the probability of obtaining an n-photon state

$$\begin{aligned} \langle n \rangle &= \langle \alpha | \, a a^\dagger \, | \alpha \rangle = |\alpha|^2 = \mu \\ P_n(\mu) &= |\langle n | \alpha \rangle|^2 = e^{-\mu} \frac{\mu^n}{n!} \end{aligned} \tag{42}$$

Moreover, the Poissonian distribution has its mean equal to the variance. Therefore, using equation 38, we obtain that the auto-correlation function for a coherent source yields

$$g^{(2)}(0) = 1 \tag{43}$$

B Beam-splitters

A beam-splitter (BS) is a passive optical device that does what it suggests by name: splits an incoming beam of light into two.

In many scenarios and applications during experimentation one can make use of a BS and they conform a basic element for almost all of our setups, being the fundamental piece for one figure of merit known as the HOM dip. That's why we think it is important to give the reader some basic notions on how it works and the properties that it unleashes when we jump to the quantum optics realm.

Firstly we will provide a classical description to get acquainted with it and then we will have to build up again our intuition to comprehend its quantum mechanical behavior.

B.1 Classical Treatment

The classical BS is a linear optical device with two input and two output ports, characterized by its intensity reflection coefficient (η). The BS acts like a partial reflector:if $\eta = 0$, the light will be completely transmitted through the device, and if it is $\eta = 1$, then the BS acts like a perfect mirror. We will use the notation shown in figure 32. The input electric field is defined as $a_{in}exp[i(2\pi\omega_0 t + \phi_{in})]$ and we will assume an ideal non-polarizing BS that has no loss and the input/output frequencies are the same.

When light enters through one of the input ports (we will use port a_{in}), the BS transforms it such that the intensities at the outputs are

$$|a|^2 = \eta|a_{in}|^2$$

$$|b|^2 = (1-\eta)|a_{in}|^2 \tag{44}$$

In the classical case, we can consider the port b_{in} to be closed and not contribute to the output. Assuming only an input in a_{in}, the outputs fields are

$$ae^{i\phi} = \sqrt{\eta}a_{in}e^{i(\phi_{in}-\phi)}$$

$$be^{i\varphi} = \sqrt{1-\eta}a_{in}e^{i(\phi_{in}-\varphi)} \tag{45}$$

And similar if we switch the ports. Alternatively, both input ports can contribute at the same time. Our next step is to determine the relative phase between the beams. If frequencies of the inputs are identical, we can write the input-output relations as

$$ae^{i\phi} = \sqrt{\eta}a_{in}e^{i(\phi_{in}-\phi)} + \sqrt{1-\eta}b_{in}e^{i(\varphi_{in}-\phi)}$$

$$be^{i\varphi} = \sqrt{1-\eta}a_{in}e^{i(\phi_{in}-\varphi)} + \sqrt{\eta}b_{in}e^{i(\varphi_{in}-\varphi)} \tag{46}$$

The relative phases are set by solving Fresnel's equations under the assumption of energy conservation, and there are multiple conventions that correspond to different mirror compositions, but we will use the convention shown in figure 32, in which the relative phase between b and b_{in} is π and the relative phase shifts of all other beams are zero

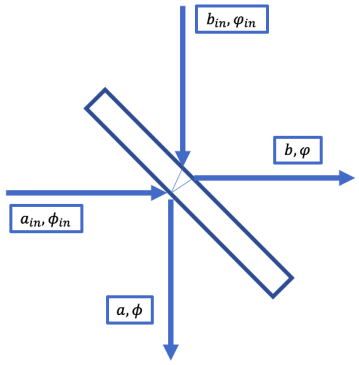

Figure 32: A diagram of a BS. a and b used for the electric fields and ϕ, φ are the phases.

$$a = \sqrt{\eta} a_{in} + \sqrt{1-\eta} b_{in}$$

$$b = \sqrt{1-\eta} a_{in} - \sqrt{\eta} b_{in} \tag{47}$$

With our phase convention set, we can move on to the transformation matrix that describes the action of the BS on the amplitudes of the input and output fields. This formalism is referred to as "input-output relations" [30]. Using equation 47, we find:

$$\begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} \sqrt{\eta} & \sqrt{1-\eta} \\ \sqrt{1-\eta} & -\sqrt{\eta} \end{bmatrix} \begin{bmatrix} a_{in} \\ b_{in} \end{bmatrix} \tag{48}$$

Now that we have characterized the non-polarizing BS, we will move on to a quantum treatment of the same element and discover some surprising differences between the behavior of light in the classical and quantum case.

B.2 Quantum Treatment

We will proceed by upgrading our fields to quantum operators creating (annihilating) single photons. Being bosons they satisfy the usual commutation relations:

$$[\hat{a}_k, \hat{a}^\dagger_{k'}] = [\hat{b}_k, \hat{b}^\dagger_{k'}] = \delta_{k,k'} \qquad [\hat{a}, \hat{b}^\dagger] = 0 \tag{49}$$

Note that we will not use hats on the operators for the rest of this section.

Let us firstly, again, consider the case where a beam a_{in} is present, and where nothing enters the other port, $b_{in} = 0$. Using equation 47, we see $a = \sqrt{\eta} a_{in}$. Let us now try and find the commutation relations of a and a_{in}:

$$[a, a^\dagger] = [\sqrt{\eta} a_{in}, \sqrt{\eta} a^\dagger_{in}] = \eta [a_{in}, a^\dagger_{in}] \quad \Longrightarrow \quad \eta = 1 \tag{50}$$

We immediately see a problem: these commutators $[a, a^\dagger]$ and $[a_{in}, a^\dagger_{in}]$ are equal to 1, so this expression sets $\eta = 1$, which is not always true. This does not imply that quantum BS are impossible to make, but rather that our theory is incomplete: one cannot consider the input b_{in} to be nonexistent as this ignores the vacuum. When we acknowledge this subtlety and write $a = \sqrt{\eta} a_{in} + \sqrt{1-\eta} b_{in}$, we find that the commutation relations are fixed:

$$[a, a^\dagger] = [\sqrt{\eta} a_{in}, \sqrt{\eta} a^\dagger_{in}] + [(\sqrt{1-\eta}) b_{in}, (\sqrt{1-\eta}) b^\dagger_{in}] =$$

$$\eta [a_{in}, a^\dagger_{in}] + (1-\eta)[b_{in}, b^\dagger_{in}] = \eta + 1 - \eta = 1 \tag{51}$$

Now, we want to find the effect of a BS in terms of a unitary matrix that acts on the photon creation and annihilation operators. That is, we want to find U_{BS} such that

$$|\Psi_{out}\rangle = U_{BS} |\Psi_{in}\rangle$$

where $|\Psi_{in}\rangle$ can be written as the state with m photons incident at a_{in} and n photons incident at b_{in}:

$$|\Psi_{in}\rangle = \frac{1}{\sqrt{n!m!}}(b_{in}^{\dagger})^{n}(a_{in}^{\dagger})^{m}\,|0\rangle_{a_{in}}\,|0\rangle_{b_{in}}$$

.

The operators of the inputs and outputs change as they go through the BS, as described by the BS matrix $a = U_{BS}^{\dagger}a_{in}^{\dagger}U_{BS}$, $b = U_{BS}^{\dagger}b_{in}^{\dagger}U_{BS}$. Let us examine the case where a single photon enters port a_{in}. We can write the action of the BS on the input state:

$$|\Psi_{out}\rangle = U_{BS}\,|\Psi_{in}\rangle = U_{BS}a_{in}^{\dagger}\,|0\rangle_{a_{in}}\,|0\rangle_{b_{in}} \tag{52}$$

We now insert the identity in the form $\mathbb{I} = U_{BS}^{\dagger}U_{BS}$:

$$U_{BS}a_{in}^{\dagger}U_{BS}^{\dagger}U_{BS}\,|0\rangle_{a_{in}}\,|0\rangle_{b_{in}} = \left(U_{BS}a_{in}^{\dagger}U_{BS}^{\dagger}\right)|0\rangle_{a}\,|0\rangle_{b} \tag{53}$$

Then, using equation 48, we find that our operators evolve as

$$U_{BS}a_{in}^{\dagger}U_{BS}^{\dagger} = \sqrt{\eta}a^{\dagger} + \sqrt{1-\eta}b^{\dagger}$$

$$U_{BS}b_{in}^{\dagger}U_{BS}^{\dagger} = \sqrt{1-\eta}a^{\dagger} - \sqrt{\eta}b^{\dagger} \tag{54}$$

and so we can continue simplifying equation 53 and find the final states of the system:

$$|\Psi_{out}\rangle = \left(U_{BS}a_{in}^{\dagger}U_{BS}^{\dagger}\right)|0\rangle_{a}\,|0\rangle_{b} = \sqrt{\eta}\,|1\rangle_{a}\,|0\rangle_{b} + \sqrt{1-\eta}\,|0\rangle_{a}\,|1\rangle_{b} \tag{55}$$

Before concluding this appendix it is worth pondering the nature of the element we have just characterized. Giving it a first look, we can see that the single photon used for the input becomes entangled with the vacuum. If we take the expectation value of the number operator $\langle\Psi_{out}|\,a^{\dagger}a\,|\Psi_{out}\rangle = \eta$ (or $1-\eta$ for the other output port) we see that the photon is in either of the outputs with the respective probabilities but not in both, as we can see from the joint number operator $\langle\Psi_{out}|\,a^{\dagger}ab^{\dagger}b\,|\Psi_{out}\rangle = 0$. The photon does not split into two, as there is no probability of finding a particle in both outputs. Another, probably more intuitive, way of looking at it is considering that the photon now is in a superposition of having taken both arms if one disregards the role of the vacuum.

C Hong-Ou-Mandel effect

The motivation for two-photon interference experiments comes from the need to characterize the output of anti-bunched light sources. As the first single photon sources appeared, laser-driven Type-1 SPDC [49, 50], one could ask the first obvious question: how similar are the states of two emitted photons? One tool that helps to characterize single photon sources is the HOM dip, a quantum interference effect that provides an effective measure of how similar the states of two emitted photons are. In many quantum communication applications a Bell-state measurement is performed assisted by this effect in a beam-splitter[10]. The characterization of indistinguishability is performed in a similar environment: two photons (or more, as we discuss in the main text), supposedly indistinguishable in all degrees of freedom are sent to a BS. Upon changing the degree of (in-)distinguishability of the photons, a signature trace will reveal itself: the HOM dip.

C.1 Photon distinguishability

Photons have degrees of freedom that allow one photon to be different from another. Let us consider the scenario where one photon enters each input port of a BS and interfere before exiting. Each photon has some characteristics, written as j and k, that can potentially distinguish it from the other. Properties j and k can be the polarization, spectrum, spatial and temporal modes. If we are working with a 50:50 BS ($\eta = \frac{1}{2}$), the evolution of our system is given by applying equation 54

$$|\Psi_{out}\rangle = U_{BS} a_j^\dagger b_k^\dagger |0\rangle_a |0\rangle_b = \left(\frac{1}{\sqrt{2}} a_j^\dagger + \frac{1}{\sqrt{2}} b_j^\dagger\right)\left(\frac{1}{\sqrt{2}} a_k^\dagger - \frac{1}{\sqrt{2}} b_k^\dagger\right) |0\rangle_a |0\rangle_b \tag{56}$$

Simplifying further, we find

$$\frac{1}{2}\left(a_j^\dagger a_k^\dagger + b_j^\dagger a_k^\dagger - a_j^\dagger b_k^\dagger - b_j^\dagger b_k^\dagger\right) |0\rangle_a |0\rangle_b \tag{57}$$

These four terms correspond to the four ways that these photons can interfere on the beamsplitter, and are represented by the images of figure 33. Note that the terms $a_j^\dagger a_k^\dagger$ and $b_j^\dagger b_k^\dagger$ (subfigures i and iv) are scenarios where one detector clicks twice and the other does not, whereas the terms $a_j^\dagger b_k^\dagger$ and $b_j^\dagger a_k^\dagger$ (subfigures ii and iii) are scenarios where both detectors click once. We define the latter event as a 'coincidence' and note that by monitoring two photon detectors, one can differentiate between coincidence and non-coincidence events.

If we take as a measurement the number of coincidence-clicks that we have at our detectors, we are able to identify between events that come from (in-)distinguishable photon interference as well as their degree of indistinguishability.

First, let us take the case where the photons are completely distinguishable (that is, $j \neq k$). We can calculate the probability of a coincidence event using Born's rule, summing the absolute value squared of the prefactors of the second and third terms. We find that the coincidence probabilility is

$$p_c = \left|\frac{1}{2}\right|^2 + \left|-\frac{1}{2}\right|^2 = \frac{1}{2} \tag{58}$$

Let us contrast this with the case where all distinguishing features are identical between the two photons (that is, $i = j$). We re-examine equation 57 and use the fact that $[b^\dagger, a^\dagger] = 0$

[10]The derivation of the BS transformation is explained in AppendixB.

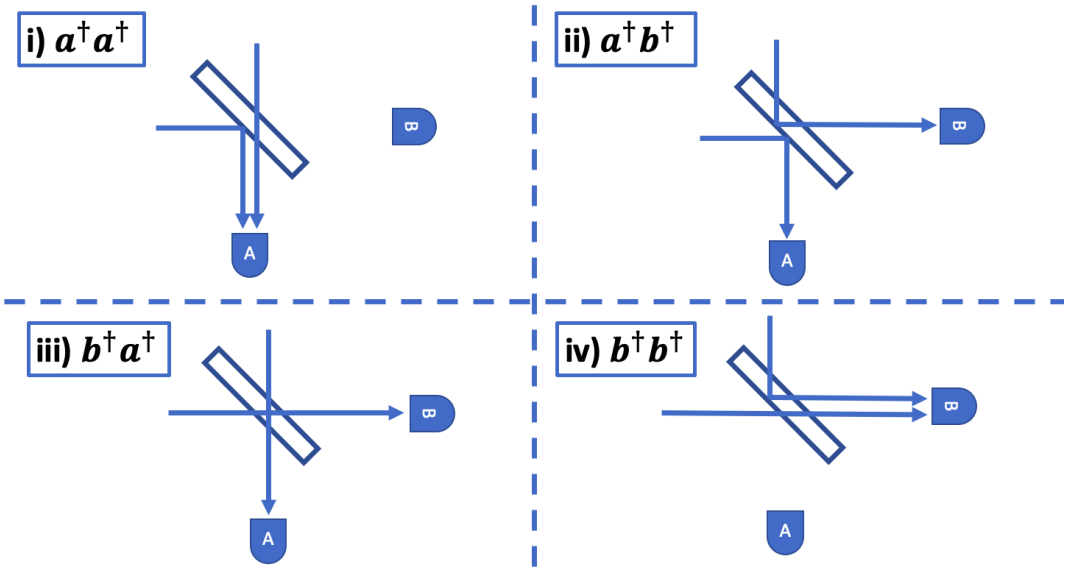

Figure 33: Each subfigure describes one way two distinguishable photons can behave on a BS. They are labeled corresponding to the four terms in equation 57. In this image one photon enters each input port and is detected at either detector a or b. Events ii and iii correspond to coincident events.

$$\frac{1}{2}\left(a^\dagger a^\dagger + b^\dagger a^\dagger - a^\dagger b^\dagger - b^\dagger b^\dagger\right)|0\rangle_a |0\rangle_b = \frac{1}{2}\left(a^\dagger a^\dagger + [b^\dagger, a^\dagger] - b^\dagger b^\dagger\right)|0\rangle_a |0\rangle_b$$

$$= \frac{1}{2}\left(a^\dagger a^\dagger - b^\dagger b^\dagger\right)|0\rangle_a |0\rangle_b = \frac{1}{\sqrt{2}}\left(|2\rangle_a |0\rangle_b - |0\rangle_a |2\rangle_b\right) \quad \Longrightarrow \quad p_c = 0 \tag{59}$$

In this case, we find a remarkable result: the coincidence probability is zero. Indeed, when the photons are identical, the probability amplitudes of the processes corresponding to subfigures ii and iii of figure 33 interfere destructively with each other [48]. Therefore, one photon goes into each input port of the BS but both must leave through the same output. This behavior seems counter-intuitive and has no classical analog.

As hinted before, by taking many of such measurements and computing the coincidence probability, one can deduce whether two photons are (in-)distinguishable. Moreover, the degree of distinguishability can be calculated by taking a HOM dip measurement. This measurement scans one of the degrees of freedom of the photons that affect distinguishability and computes the coincidence probability.

Let's now analyze these four degrees of freedom and their effect on the measurement and coincidence probability [51].

- **Polarization**

One characteristic of light is its polarization. The electromagnetic field has two orthogonal polarizations, and one can distinguish between the two using a polarizing filter. If one were to input horizontally polarized light into one input of a BS and vertically polarized light into the other, one would measure a coincidence probability of 0.5. However, if the vertically polarized light is tuned towards horizontal,

the coincidence probability would drop towards zero. The math for the limit cases H and V is exactly analogous as shown in equation 59. Any polarization in between would show a reduced coincidence probability.

- **Temporal distinguishability**

Another property that can distinguish photons is their time of arrival at the BS. If two identical photons exit a photon source, but the two travel for very different distances before reaching the beamsplitter, the two photons will not interfere. This path-length difference can be characterized by a delay time τ. Our goal now is to calculate the coincidence probability as a function of the delay time - this is the relation measured in Hong, Ou, and Mandel's original 1987 experiment.

In order to do so we must consider the spectral amplitude function of the photons. As the delay time is varied, these functions will change their overlap, which determines the coincidence probability. For now, we will consider the case where both photons have the same spectral amplitude function, $\phi(\omega)$. We can consider the path lengths to the input spatial modes a and b of the beasmplitter; this will be represented by the phase $e^{-i\omega\tau}$ and can be viewed as a difference in the arrival time of the two wave-packets at the beamsplitter. We begin by calculating the time-delayed input state before the beamsplitter transformation:

$$|\Psi_{in}\rangle = \int d\omega_1 \phi(\omega_1) a_{in}^{\dagger}(\omega_1) \int d\omega_2 \phi(\omega_2) b_{in}^{\dagger}(\omega_2) e^{-i\omega_2\tau} |0\rangle |0\rangle \tag{60}$$

The calculation is a bit too long to write out in full, but the individual steps are covered in Section 4.1 of [51]. One applies the unitary operators from equation 54 as before and projects the result onto states where one photon is present at each detector, $P_a \otimes P_b$. The coincidence probability is calculated as $p_c = \langle \Psi_{in} | U_{BS}^{\dagger} P_a \otimes P_b U_{BS} | \Psi_{in} \rangle$, which yields

$$p_c = \frac{1}{2} - \frac{1}{2} \int d\omega_1 \left|\phi\left(\omega_1\right)\right|^2 \mathrm{e}^{-i\omega_1\tau} \int d\omega_2 \left|\phi\left(\omega_2\right)\right|^2 \mathrm{e}^{i\omega_2\tau} \tag{61}$$

If we only want to take into account the relevance of the time delay, we can set the central frequencies $\omega_1 = \omega_2$ and give the photons a spectral lineshape $\phi(\omega)$ that is a normalized Gaussian with width σ. This leads to

$$p_c = \frac{1}{2} - \frac{1}{2} e^{-\frac{\sigma^2\tau^2}{2}} \tag{62}$$

Extreme cases of this result are easily checked: as we decrease the delay time to zero, the photons are completely identical when they interfere on the BS and we find that the coincidence probability drops to zero; when the delay time grows large, the coincidence probability tends towards $\frac{1}{2}$, as expected. Of course, one can plug in different spectral profiles of photon wave-packets and retrieve different expressions for the coincidence probability.

As a result, when one measures the coincidence probability against the delay time, one gains information about the spectral amplitude function.

- **Spatial and Spectral Profile**

Now assume that photons arrive at the BS as wave-packets that have some transverse spatial mode as well as a spectral lineshape. One can measure the HOM effect using the spatial or spectral profile as the distinguishable property.

Taking a general function for the photons' amplitude function $f(\omega_1, \omega_2)$ we can follow the same derivations as before to yield the general case

$$p_c = \frac{1}{2} - \frac{1}{2}\int d\omega_1 \int d\omega_2 f^*(\omega_1,\omega_2)\, f(\omega_2,\omega_1)\, e^{i(\omega_2-\omega_1)\tau} \tag{63}$$

If we were to consider $f(\omega_1,\omega_2) = \phi(\omega_1)\varphi(\omega_2)$ (independent and separable) we automatically recover a similar result as 61 but now with two different spectral amplitude functions.

However, what if the spectral amplitudes are entangled, very much like in SPDC processes and their Joint Spectral Amplitude (JSA)[51]. This calculation is not easy because joint spectral amplitudes are not typically simple expressions. However, using numerical integration and some approximations one can find that entangled photons have a different coincidence probability function than non-entangled photons. In fact, one can even distinguish between different entangled spectra. For example, the shape of the Hong-Ou Mandel dip using SPDC pumped by a pulsed laser to generate photons is different from the HOM dip in an experiment that uses a continuous wave laser instead [51].

C.2 Hong-Ou-Mandel experiments

The figure or merit obtained by HOM-dip experimental setups is the measurement of the coincidence probability function, shown in figure 34 which, in turn, yields the HOM visibility. This is done by gradually modifying one degree of freedom of the input photons and therefore changing their distinghuishability; and and detecting the coincidence events. Adding temporal delay to one of the pulses is usually one of the easiest parameters to scan. In the original paper [50], this delay was induced by a piezoelectric transducer that had a minimum shift of about 1 micron, which allowed for shifts in the beam path that correspond to time delay shifts on the order of femtoseconds. There are two other features of the dip that are usually measured and discussed. Firstly the shape and width. This feature indicates the region in which the photons have some degree of indistinguishability. The other feature is the visibility, or the relative height, $V = \frac{h_{max}-h_{min}}{h_{max}}$, of the HOM dip. The dotted line in figure 34 corresponds to a fitted Lorentzian with 90% visibility.

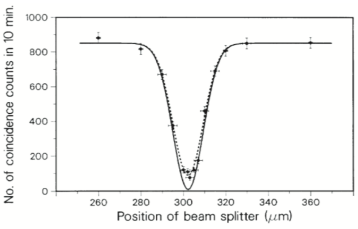

Figure 34: HOM dip trace obtained by Hong, Ou, and Mandel [50].

In this section we have described that different properties of photons can lead to different interference effects and learned how to calculate the coincidence probability function, otherwise known as the Hong-Ou-Mandel dip. The dip contains information about the temporal, spatial, spectral, and entanglement characteristics of the light impinging onto the BS, which is why it has been such a useful tool in quantum optics and is so often repeated.

References

[1] Richard Jozsa, Daniel S Abrams, Jonathan P Dowling, and Colin P Williams. Quantum clock synchronization based on shared prior entanglement. *Physical Review Letters*, 85(9):2010, 2000.

[2] Hoi-Kwong Lo, Marcos Curty, and Bing Qi. Measurement-device-independent quantum key distribution. *Physical review letters*, 108(13):130503, 2012.

[3] Raju Valivarthi, Marcel.li Grimau Puigibert, Qiang Zhou, Gabriel H. Aguilar, Varun B. Verma, Francesco Marsili, Matthew D. Shaw, Sae Woo Nam, Daniel Oblak, and Wolfgang Tittel. Quantum teleportation across a metropolitan fibre network. *Nature Photonics*, 10(10):676–680, October 2016.

[4] Zeng-Bing Chen, Bo Zhao, Yu-Ao Chen, Jörg Schmiedmayer, and Jian-Wei Pan. Fault-tolerant quantum repeater with atomic ensembles and linear optics. *Physical Review A*, 76(2):022329, 2007.

[5] W Dür, H-J Briegel, J Ignacio Cirac, and P Zoller. Quantum repeaters based on entanglement purification. *Physical Review A*, 59(1):169, 1999.

[6] Koji Azuma, Kiyoshi Tamaki, and Hoi-Kwong Lo. All-photonic quantum repeaters. *Nature communications*, 6:6787, 2015.

[7] Zheng-Da Li, Rui Zhang, Xu-Fei Yin, Li-Zheng Liu, Yi Hu, Yu-Qiang Fang, Yue-Yang Fei, Xiao Jiang, Jun Zhang, Feihu Xu, et al. Experimental demonstration of all-photonic quantum repeater. In *CLEO: QELS_Fundamental Science*, pages FTh4A–6. Optical Society of America, 2019.

[8] Neil Sinclair, Erhan Saglamyurek, Hassan Mallahzadeh, Joshua A Slater, Mathew George, Raimund Ricken, Morgan P Hedges, Daniel Oblak, Christoph Simon, Wolfgang Sohler, et al. Spectral multiplexing for scalable quantum photonics using an atomic frequency comb quantum memory and feed-forward control. *Physical review letters*, 113(5):053603, 2014.

[9] Donald F Swinehart. The beer-lambert law. *Journal of chemical education*, 39(7):333, 1962.

[10] Marcus W Doherty, Neil B Manson, Paul Delaney, Fedor Jelezko, Jörg Wrachtrup, and Lloyd CL Hollenberg. The nitrogen-vacancy colour centre in diamond. *Physics Reports*, 528(1):1–45, 2013.

[11] Daniel Loss and David P DiVincenzo. Quantum computation with quantum dots. *Physical Review A*, 57(1):120, 1998.

[12] T Ferreira Da Silva, D Vitoreti, GB Xavier, GC Do Amaral, GP Temporao, and JP Von Der Weid. Proof-of-principle demonstration of measurement-device-independent quantum key distribution using polarization qubits. *Physical Review A*, 88(5):052303, 2013.

[13] JE Mooij, TP Orlando, L Levitov, Lin Tian, Caspar H Van der Wal, and Seth Lloyd. Josephson persistent-current qubit. *Science*, 285(5430):1036–1039, 1999.

[14] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. Quantum cryptography. *Reviews of Modern Physics*, 74(1):145–195, Mar 2002.

[15] Jürgen Brendel, Nicolas Gisin, Wolfgang Tittel, and Hugo Zbinden. Pulsed energy-time entangled twin-photon source for quantum communication. *Physical Review Letters*, 82(12):2594, 1999.

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

[17] Charles H Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. *arXiv preprint arXiv:2003.06557*, 2020.

[18] Norbert Lütkenhaus and Mika Jahma. Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack. *New Journal of Physics*, 4:44–44, jul 2002.

[19] Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen. Decoy state quantum key distribution. *Physical review letters*, 94(23):230504, 2005.

[20] Daniel Gottesman, H-K Lo, Norbert Lutkenhaus, and John Preskill. Security of quantum key distribution with imperfect devices. In *International Symposium onInformation Theory, 2004. ISIT 2004. Proceedings.*, page 136. IEEE, 2004.

[21] Marco Lucamarini, Zhiliang L Yuan, James F Dynes, and Andrew J Shields. Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. *Nature*, 557(7705):400–403, 2018.

[22] Xiongfeng Ma. Quantum cryptography: theory and practice, 2008.

[23] Paul G Kwiat and Harald Weinfurter. Embedded bell-state analysis. *Physical Review A*, 58(4):R2623, 1998.

[24] Warren P Grice. Arbitrarily complete bell-state measurement using only linear optical elements. *Physical Review A*, 84(4):042331, 2011.

[25] Yoon-Ho Kim, Sergei P Kulik, and Yanhua Shih. Quantum teleportation of a polarization state with a complete bell state measurement. *Physical Review Letters*, 86(7):1370, 2001.

[26] I Marcikic, H De Riedmatten, W Tittel, H Zbinden, and N Gisin. Long distance quantum teleportation of qubits from photons at 1300 nm to photons at 1550 nm wavelength. *arXiv preprint quant-ph/0301178*, 2003.

[27] Hugues de Riedmatten, Ivan Marcikic, JAW Van Houwelingen, Wolfgang Tittel, Hugo Zbinden, and Nicolas Gisin. Long-distance entanglement swapping with photons from separated sources. *Physical Review A*, 71(5):050302, 2005.

[28] Matthew J Collins, Chunle Xiong, Isabella H Rey, Trung D Vo, Jiakun He, Shayan Shahnia, Christopher Reardon, Thomas F Krauss, MJ Steel, Alex S Clark, et al. Integrated spatial multiplexing of heralded single-photon sources. *Nature communications*, 4(1):1–7, 2013.

[29] Chunle Xiong, X Zhang, Z Liu, Matthew J Collins, A Mahendra, LG Helt, Michael J Steel, D-Y Choi, CJ Chae, PHW Leong, et al. Active temporal multiplexing of indistinguishable heralded single photons. *Nature communications*, 7(1):1–6, 2016.

[30] Christopher Gerry, Peter Knight, and Peter L Knight. *Introductory quantum optics*. Cambridge university press, 2005.

[31] Yasser Jeronimo-Moreno, Saul Rodriguez-Benavides, and Alfred B U'Ren. Theory of cavity-enhanced spontaneous parametric downconversion. *Laser physics*, 20(5):1221–1233, 2010.

[32] Peng Cheng Wang. A demonstration of frequency conversion and shifting technology for frequency multiplexed quantum repeaters. Master's thesis, TU Delft, 2019.

[33] M. Falamarzi Askarani. *Telecom-wavelength quantum memories in rare earth ion-doped materials for quantum repeaters*. Delft University of Technology, 2019.

[34] M Grimau Puigibert, GH Aguilar, Q Zhou, F Marsili, MD Shaw, VB Verma, SW Nam, D Oblak, and W Tittel. Heralded single photons based on spectral multiplexing and feed-forward control. *Physical Review Letters*, 119(8):083601, 2017.

[35] Lora Nugent-Glandorf, Tyler Neely, Florian Adler, Adam J Fleisher, Kevin C Cossel, Bryce Bjork, Tim Dinneen, Jun Ye, and Scott A Diddams. Mid-infrared virtually imaged phased array spectrometer for rapid and broadband trace gas detection. *Optics letters*, 37(15):3285–3287, 2012.

[36] Xinrong Hu, Qiang Sun, Jing Li, Chun Li, Ying Liu, and Jianzhong Zhang. Spectral dispersion modeling of virtually imaged phased array by using angular spectrum of plane waves. *Optics Express*, 23(1):1–12, 2015.

[37] Shijun Xiao, Andrew M Weiner, and Christopher Lin. Experimental and theoretical study of hyperfine wdm demultiplexer performance using the virtually imaged phased-array (vipa). *Journal of lightwave technology*, 23(3):1456, 2005.

[38] Scott A Diddams, Leo Hollberg, and Vela Mbele. Molecular fingerprinting with the resolved modes of a femtosecond laser frequency comb. *Nature*, 445(7128):627–630, 2007.

[39] *Driving EO Phase Modulators*.

[40] Agata M Brańczyk. Hong-ou-mandel interference. *arXiv preprint arXiv:1711.00080*, 2017.

[41] Eleftherios Moschandreou, Jeffrey I Garcia, Brian J Rollick, Bing Qi, Raphael Pooser, and George Siopsis. Experimental study of hong–ou–mandel interference using independent phase randomized weak coherent states. *Journal of Lightwave Technology*, 36(17):3752–3759, 2018.

[42] Allison Rubenok, Joshua A Slater, Philip Chan, Itzel Lucio-Martinez, and Wolfgang Tittel. Real-world two-photon interference and proof-of-principle quantum key distribution immune to detector attacks. *Physical review letters*, 111(13):130501, 2013.

[43] Xiang-Bin Wang. Three-intensity decoy-state method for device-independent quantum key distribution with basis-dependent errors. *Physical Review A*, 87(1):012320, 2013.

[44] Raju Valivarthi, Qiang Zhou, Gabriel H Aguilar, Varun B Verma, Francesco Marsili, Matthew D Shaw, Sae Woo Nam, Daniel Oblak, Wolfgang Tittel, et al. Quantum teleportation across a metropolitan fibre network. *Nature Photonics*, 10(10):676–680, 2016.

[45] JG Rarity, PR Tapster, and R Loudon. Non-classical interference between independent sources. *arXiv preprint quant-ph/9702032*, 1997.

[46] Mark Fox. *Quantum optics: an introduction*, volume 15. OUP Oxford, 2006.

[47] U. M. Titulaer and R. J. Glauber. Correlation functions for coherent fields. *Phys. Rev.*, 140:B676–B682, Nov 1965.

[48] D. F. Walls and G. J. Milburn. *Quantum optics / D.F. Walls, G.J. Milburn*. Springer-Verlag Berlin ; New York, springer study ed. edition, 1995.

[49] Gilbert Grynberg, Alain Aspect, and Claude Fabre. *Introduction to quantum optics: from the semi-classical approach to quantized light*. Cambridge university press, 2010.

[50] Chong-Ki Hong, Zhe-Yu Ou, and Leonard Mandel. Measurement of subpicosecond time intervals between two photons by interference. *Physical review letters*, 59(18):2044, 1987.

[51] Agata M Brańczyk. Hong-ou-mandel interference. *arXiv preprint arXiv:1711.00080*, 2017.