KØBENHAVNS UNIVERSITET
DET NATUR- OG BIOVIDENSKABELIGE FAKULTET

MASTER'S THESIS

Study of InGaAs quantum dots as single-photon sources for Device-Independent Quantum Key Distribution

Eva María González Ruiz

Supervised by
Anders S. Sørensen

Co-supervised by
Sumanta K. Das

Submitted on the 3rd of September 2019

This page is intentionally left blank.

Abstract

A loophole-free violation of Bell's inequality is required for Device-Independent Quantum Key Distribution (DIQKD) protocols to work, requiring a certain efficiency of the source. Both the locality and detection loopholes must be closed; however, while closing the locality loophole only requires ensuring a determined distance between Alice and Bob, the detection loophole demands very high transmission efficiencies [1]. To overcome it, we have introduced a heralding scheme proposed by [2] that, furthermore, creates entanglement by measurement between the pair of photons shared by Alice and Bob, thus avoiding the potential action of the eavesdropper on the state. We have studied the reliability of InGaAs quantum dots as single-photon sources for the completion of the protocol, with the intention of implementing DIQKD based on them in the near future. We have analyzed both the influence of distinguishability and losses, together with the limitations in the resolution of the number of photons in the detection. We have studied the effect of the distinguishability of photons by relating it to the HOM visibility of the sources, finding a threshold of $V \approx 79\%$. This visibility is accomplishable by InGaAs quantum-dot single-photon sources [3]. However, the relation obtained between the local efficiency and the required visibility shows that the necessary local efficiencies ($\eta_l \approx 90\%$) are yet not achievable with current photonic implementations [4]. Finally, we have aimed to find the best compromise between a high heralding rate and the probability of receiving incorrect messages of success from the heralding station by optimizing the probability of transmission T of the local beam splitters. We find that the optimal probability of transmission decreases with the distinguishability of photons. Our results show that the necessary experimental time to accomplish the violation of Bell's inequality with several standard deviations is not unreasonable.

Acknowledgments

I find it very special to have the opportunity of expressing my gratitude towards all the important people that have supported me throughout this year. I really hope I can transmit how immensely fortunate I feel for having each and every one of you in my life in one or another way.

I have trouble putting into words how essential my family is for me. I simply owe every single minute of the privilege of studying in Copenhagen to the trust and support that my parents have always given me. Having been able to overcome all the challenges that this year has put me on the road would have been unthinkable without them. Finishing this stage is just one more step in a process that began since they were patiently answering all my questions as a child, always inviting me to keep on challenging myself. *Gracias por apoyarme en todas mis decisiones y, sobre todo, por enseñarme a ser feliz.*

I feel very honored for having had the opportunity to work under the supervision of Anders Sørensen. Beyond the obvious fact that I would have not been able to accomplish this thesis without his patient advice, I have to thank him for making me re-discover how exciting and fascinating research can be. His motivating guidance has been fundamental to help me enjoy this work even in the hardest moments. *Jeg vil også gerne takke ham for hans tålmodighed med mit dårlig dansk.*

I also want to thank the support and advice of Sumanta Das all along the way, for his ideas and helpful guidance in the development of the thesis. I feel very grateful for his supervision during this year, and especially with the writing of the thesis in the intense last weeks. Thanks to Johann and Freja for also taking the time to proofread the physics of the project. Finally, I also feel very thankful for my SymfUni friends Estelle, Liv, Mai, Jeppe, Kyle, Leif, and Raúl, for criticizing my written *spanglish*, not to mention all the great moments we have had together.

Finally, I want to thank Peter Lodahl for suggesting this project in the first place, I hope our contribution can be useful for future research at the Nanophotonics group. I really appreciate being part of Hy-Q, and I feel very fortunate for having shared my days with so many amazing people in such an enriching atmosphere.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

This chapter presents the fundamental theoretical background of the thesis. Its heterogeneity responds to the need of introducing very different topics and tools that are nevertheless relevant for the correct understanding of the following chapters. Bell's inequality and the challenges that its experimental violation implies are presented, followed by an introduction to Quantum Key Distribution (QKD) and, particularly, both the advantages and experimental difficulties of Device-Independent QKD implementations. We next explain the Hong-Ou-Mandel effect, as it is the main concept underlying the scheme of the set-up we will work with. Finally, the basic concepts of density matrix tomography are outlined.

1.1 Bell's inequality

The beginning of the 20th century was incredibly fascinating for the development of what, nowadays, we call modern physics. The contributions from Hilbert and Dirac in the early 30s gave the final form and structure to a whole new frame of work in the form of the quantum mechanics theory. This new paradigm was, by this date, far more consolidated compared to the first approaches and ideas developed by Max Planck that awarded him with the Nobel Prize in 1918. However, despite the incipient irrefutable experimental success of quantum mechanics, the decade of the 1930s was also the starting point of deeper discussions, even more focused on the philosophical plane, regarding the nature of quantum theory. They opened a debate that has last for almost a century. In 1935, Einstein, Podolsky, and Rosen (EPR) published the famous paper "Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?" [6], where they claimed that a local realist[1] read of quantum theory is not compatible with its basic principles. Unless immediate effects between quantum correlated systems occur, thus violating relativity, EPR showed that Heisenberg uncertainty principle is violated. Thus, although not incorrect, the description that quantum mechanics provides is certainly incomplete, opening the door to hidden variables that could, in fact, determine these spooky correlations.

A more approachable interpretation of this so-called EPR Paradox was made by Bohm and Aharonov in 1957 [8]. Let us imagine a spin-0 particle decaying into two identical spin one-half

[1] A realist theory implies that the measurement outcomes after the observation of a system are not influenced by the measurement itself, but are determined beforehand instead. On the other hand, a theory is considered local if the outcome of the measurement performed over a system is independent of another distant system that had interacted with it in the past [7].

particles that move away from each other. The conservation of the total spin forces the sum of the projection of the two emmitted particles to equal 0 as well. The shared state $|\psi\rangle$ between the two subsystems is an *entangled* state[2], meaning that it can not be written as a product state of its two different components (in which case would be separable):

$$\left|\psi^-\right\rangle = \frac{1}{\sqrt{2}}\left(|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle\right) . \tag{1.1}$$

If the spin of the first particle is measured along any axis, there is a 50% probability that the outcome will be ↑ or ↓. However, after that measurement is done, if the spin of the second particle is afterwards measured over the same axis, the outcome is unequivocally determined: as the total spin must be zero, if the first particle measured ↑ then the second must show ↓, and viceversa. A measurement of the spin of the second particle over a perpendicular axis to the one that was used with the first particle, however, would have again a 50% probability of obtaining one or another outcomes. This shows the existence of an obvious correlation between both distant particles: the nature of this correlation is, however, the main point of the EPR paradox. Quantum mechanics would be a realist theory if the measurement outcomes were prefixed. Otherwise, the measurement of the first particle would influence non-locally over the observation of the second one. Non-local correlations would exists between entangled subsystems.

1.1.1 The CHSH Inequality

It was not until 1964 when J. Bell suggested to extend Bohm's approach to measurements in any direction, and study the nature of the correlations [7]. His premise was to assume local determinism in his result, which made him arrive to the so-called Bell inequality. Whether the quantum mechanical predictions violate the inequality or not would shed light into the nature of quantum correlations. Instead of following his original work, we have followed for simplicity the result obtained by J. Clauser, M. Horne, A. Shimony y R. Holt in 1969 (as well as references [9], [10] and [11]), who developed an alternative version of the original inequality suggested by Bell, in order to test Bell inequality experimentally [12]. Let us consider that Alice and Bob can measure two observables (for example, again, the polarization of two photons), $\mathbf{a}$ and $\mathbf{a}'$, and $\mathbf{b}$ and $\mathbf{b}'$ respectively, which can take the values $\{\pm1\}$. If we assume local realism, Alice and Bob should be able to measure both of their observables and the outcomes would not be influenced in any case by the others. Under this assumption, note that the product of any observable will also take the values $\{\pm1\}$, and thus we can construct the following expression:

$$\mathbf{ab} + \mathbf{a}'\mathbf{b} + \mathbf{ab}' - \mathbf{a}'\mathbf{b}' = \mathbf{a}(\mathbf{b}+\mathbf{b}') + \mathbf{a}'(\mathbf{b}-\mathbf{b}') = \pm 2\,. \tag{1.2}$$

Note that $\mathbf{b}+\mathbf{b}'$ can either equal 2, -2 or 0. If it equals ±2, then $\mathbf{b}-\mathbf{b}'=0$; if on the contrary $\mathbf{b}+\mathbf{b}'=0$, then $\mathbf{b}-\mathbf{b}'=\pm2$. Therefore we can conclude that equation 1.2 can only take the values ±2. We can apply now the integral form of the well known triangle inequality[3], by taking the expectation value of 1.2. In fact:

$$S \equiv |\langle \mathbf{ab} + \mathbf{a}'\mathbf{b} + \mathbf{ab}' - \mathbf{a}'\mathbf{b}' \rangle| = |\langle \mathbf{ab}\rangle + \langle \mathbf{a}'\mathbf{b}\rangle + \langle \mathbf{ab}'\rangle - \langle \mathbf{a}'\mathbf{b}'\rangle| \leq \langle |\mathbf{ab} + \mathbf{a}'\mathbf{b} + \mathbf{ab}' - \mathbf{a}'\mathbf{b}'|\rangle = 2\,, \tag{1.3}$$

[2]The state $\left|\psi^-\right\rangle$ is in fact one of the four Bell states, $\left|\psi^\pm\right\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle \pm |10\rangle\right)$ and $\left|\phi^\pm\right\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle \pm |11\rangle\right)$, which constitute a basis of maximally entangled states.

[3]$|\int f(x)dx| \leq \int |f(x)|dx$

which is known as the CHSH Inequality. We should remark that this result is completely general and applies to any local realist theory, so the next question would be: what if we calculate the expectation values of the observables quantum-mechanically? Let Alice and Bob share a maximally entangled state, for example, of two photons with orthogonal polarizations $|{\rightarrow}\rangle$ and $|{\uparrow}\rangle$. For simplicity in the calculation, we choose the state $|\psi^-\rangle = \frac{1}{\sqrt{2}}\left(|{\rightarrow\uparrow}\rangle - |{\uparrow\rightarrow}\rangle\right)$ because it is invariable under rotations, but it can be proven that *any* entangled pure state violates Bell inequality [11]. In order to define operators with the same eigenvalues as the observables of the situation described above, let us just define a general hermitian operator written in terms of the Pauli matrices, where $\hat{n}_A$ and $\hat{n}_B$ are unitary vectors that designate the projection that Alice and Bob make with their measurement:

$$\mathbf{a} = \hat{\mathbf{n}}_A \hat{\boldsymbol{\sigma}}_A, \quad \mathbf{a}' = \hat{\mathbf{n}}'_A \hat{\boldsymbol{\sigma}}_A, \quad \mathbf{b} = \hat{\mathbf{n}}_B \hat{\boldsymbol{\sigma}}_B, \quad \mathbf{b}' = \hat{\mathbf{n}}'_B \hat{\boldsymbol{\sigma}}_B\,, \tag{1.4}$$

then we can calculate the expectation value

$$\langle \mathbf{ab} \rangle = \left\langle \psi^- \right| \mathbf{a} \otimes \mathbf{b} \left| \psi^- \right\rangle = \left\langle \psi^- \right| \left(\hat{\mathbf{n}}_A \hat{\boldsymbol{\sigma}}_A\right) \otimes \left(\hat{\mathbf{n}}_B \hat{\boldsymbol{\sigma}}_B\right) \left| \psi^- \right\rangle . \tag{1.5}$$

As we mentioned above, $|\psi^-\rangle$ is rotational invariant or, in other words, it is invariant under the action of a general rotation operator $R(\theta)$, that can be written without loss of generality in terms of the Pauli matrices [10]:

$$\begin{aligned} R(\theta)_A \otimes R(\theta)_B \left|\psi^-\right\rangle = \left|\psi^-\right\rangle &\Leftrightarrow \left(\cos\frac{\theta}{2}\mathbb{1} - i\sin\frac{\theta}{2}\hat{\mathbf{n}}\hat{\boldsymbol{\sigma}}_A\right) \otimes \left(\cos\frac{\theta}{2}\mathbb{1} - i\sin\frac{\theta}{2}\hat{\mathbf{n}}\hat{\boldsymbol{\sigma}}_B\right)\left|\psi^-\right\rangle = \left|\psi^-\right\rangle \\ &\Leftrightarrow -i\sin\frac{\theta}{2}\cos\frac{\theta}{2}\left(\hat{\mathbf{n}}\hat{\boldsymbol{\sigma}}_A + \hat{\mathbf{n}}\hat{\boldsymbol{\sigma}}_B\right)\left|\psi^-\right\rangle = 0 \\ &\Leftrightarrow \left(\hat{\boldsymbol{\sigma}}_A + \hat{\boldsymbol{\sigma}}_B\right)\left|\psi^-\right\rangle = 0 \\ &\Leftrightarrow \hat{\boldsymbol{\sigma}}_A\left|\psi^-\right\rangle = -\hat{\boldsymbol{\sigma}}_B\left|\psi^-\right\rangle . \end{aligned} \tag{1.6}$$

With this result, we can write the expectation value from equation 1.5 as the trace of the reduced density matrix of only one of the subsystems. For instance, Alice's $\hat{\rho}_A$:

$$\langle \mathbf{ab} \rangle = -\left\langle \psi^- \right| \left(\hat{\mathbf{n}}_A \hat{\boldsymbol{\sigma}}_A\right)\left(\hat{\mathbf{n}}_B \hat{\boldsymbol{\sigma}}_A\right)\left|\psi^-\right\rangle = -\operatorname{Tr}\{\left(\hat{\mathbf{n}}_A \hat{\boldsymbol{\sigma}}_A\right)\left(\hat{\mathbf{n}}_B \hat{\boldsymbol{\sigma}}_A\right)\hat{\rho}_A\}\,. \tag{1.7}$$

Recall that the reduced density matrix is calculated as the partial trace over the other subsystem, which for a maximally entangled state yields $\frac{1}{2}\mathbb{1}$, as each of the subsystems do not have any information accesible over the whole state:

$$\hat{\rho}_A = \operatorname{Tr}_B \hat{\rho} = \operatorname{Tr}_B \left|\psi^-\right\rangle\left\langle\psi^-\right| = \frac{1}{2}\mathbb{1}\,. \tag{1.8}$$

Thus, continuing with equation 1.7:

$$\begin{aligned} \langle \mathbf{ab} \rangle &= -\frac{1}{2}\operatorname{Tr}\{\left(\hat{\mathbf{n}}_A \hat{\boldsymbol{\sigma}}_A\right)\left(\hat{\mathbf{n}}_B \hat{\boldsymbol{\sigma}}_A\right)\} = -\frac{1}{2}\sum_{ij}\operatorname{Tr}\left\{\left(\hat{n}_{A_i}\hat{\sigma}_{A_i}\right)\left(\hat{n}_{B_j}\hat{\sigma}_{A_j}\right)\right\} \\ &= -\frac{1}{2}\sum_{ij}\hat{n}_{A_i}\hat{n}_{B_j}\operatorname{Tr}\left\{\hat{\sigma}_{A_i}\hat{\sigma}_{A_j}\right\} = -\frac{1}{2}\sum_{ij}\hat{n}_{A_i}\hat{n}_{B_j}\left(\operatorname{Tr}\{\delta_{ij}\mathbb{1}\} + i\epsilon_{ijk}\operatorname{Tr}\{\sigma_k\}\right) \\ &= -\sum_{ij}\hat{n}_{A_i}\hat{n}_{B_j}\delta_{ij} = -\hat{\mathbf{n}}_A\hat{\mathbf{n}}_B\,. \end{aligned} \tag{1.9}$$

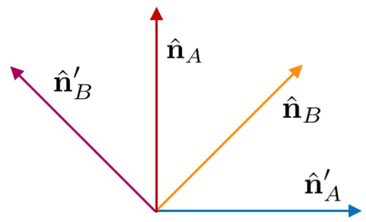

Figure 1.1: Choice of measurement axis $\hat{\mathbf{n}}_A$, $\hat{\mathbf{n}}_B$, $\hat{\mathbf{n}}'_A$ and $\hat{\mathbf{n}}'_B$ with which the maximal violation of the CHSH inequality is achieved.

Therefore we have found that, according to quantum mechanics, the outcomes of the observables $\mathbf{a}$ and $\mathbf{b}$ are anticorrelated and depend on the angle θ, defined as the one between the chosen measurement axis $\hat{\mathbf{n}}_A$ and $\hat{\mathbf{n}}_B$:

$$\langle \mathbf{ab} \rangle = -\cos\theta \,. \tag{1.10}$$

If we choose the angles for the measurement axis such that they are restricted to be coplanar for simplicity, that is considering an angle of $\pi/4$ between each of them (the Bell angles), as sketched in Figure 1.1, we get:

$$\begin{aligned} S &= |\langle \mathbf{ab} \rangle + \langle \mathbf{a'b} \rangle + \langle \mathbf{ab'} \rangle - \langle \mathbf{a'b'} \rangle| = |-\cos\frac{\pi}{4} - \cos\frac{\pi}{4} - \cos\frac{\pi}{4} - (-\cos\frac{3\pi}{4})| \\ &= |-3\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}| = 2\sqrt{2} > 2 \,. \end{aligned} \tag{1.11}$$

The quantum state $|\psi^-\rangle$ exhibits a clear violation of the CHSH inequality. This has very important implications in the fundamental understanding of quantum mechanics: if one assumes that quantum theory is deterministic and local, reaches a contradiction. The only way to be able to understand the outcomes of measurements as prefixed would be in a frame of non-locality. If, as Einstein, Podolsky and Rosen claimed, quantum mechanics is incomplete, it is not only incomplete but also wrong. Any theory of local hidden variables is incompatible with the predictions of quantum mechanics.

1.1.2 Experimental challenges: loopholes in Bell tests

Verifying experimentally the violation of Bell's inequality is, however, very demanding. The experimental circumstances in which Bell tests are carried out, might force further assumptions, and thus local realism could in principle provide with a correct prediction of the outcome of the measurements too [13]. This is known as *loopholes*, and we will briefly relate the most significant ones as well as review some of the most outstanding results so far.

If Alice and Bob are not placed sufficiently far apart, subluminal communication could be allowed between them, providing each other with information about the choice of measurement axis they make. In addition, if this choice is made before the experiment starts the assumption of non-locality is not ensured either. This is known as the *locality loophole*. Therefore the measurement settings have to be decided in a time window smaller than the time it takes photons to travel between Alice and Bob. The first experiment to achieve it was made by Aspect, Grangier and Roger in 1982 [14], based on the interpretation of Bell's inequality made by Bohm and Aharonov, as they used analyzers that varied in a shorter time compared with the flying time of the photon.

It was published only several months after a previous experimental attempt was also concluded [15], in which they did not focus on the locality loophole. However, the detection efficiency of these experiments was not sufficiently high so as to avoid the *detection loophole*. This loophole arises from the fact that one has to be able to identify each experimental run, so it is possible to distinguish which runs correspond to undetected-photon events. Otherwise, it is not possible to indentify the events properly, thus invaliding Bell's inequality. If the experimental runs are identifiable, in principle, one could think of making a fair-sampling assumption and disregard all those events in which photons were not detected. However, this is not possible either, as making that assumption takes for granted that the plausible local hidden variable is not influencing which photons are detected and which not, and this is something that the hidden variable could definitely do. Therefore only experiments with sufficiently high efficiency of detection (from the generation of the photon until the detection itself) can close the detection loophole. For the CHSH inequality, this efficiency threshold is proven to be $\eta \approx 82.84\%$ [16], and it varies for other versions of Bell's inequality [17]. In particular, one can develop inequalities already free from the fair-sampling assumption that can lower the efficiency threshold. Eberhard's inequality [18] incorporates undetected-photon events to its derivation, establishing a required efficiency of $2/3 \approx 66.67\%$ by using non-maximally entangled states. After many years in which experiments closed either one or the other loopholes, both detection and locality ones were closed simultaneously for the first time in three different experiments in 2015: the ones carried out by Giustina et al. [19] and Shalm et al. [20], with photons generated by parametric-down conversion and superconducting detectors and by Hensen et al., with electron spins [21]. Finally, note that to have a completely loophole free Bell test, one also have to close the *coincidence-time*, *freedom of choice* and *memory* loopholes [22]. We will not focus on these ones in this present work.

1.2 Quantum Cryptography

Cryptography has experienced an important development over the past century, mostly focused on public key systems like the asymmetric RSA (Rivest–Shamir–Adleman). These kind of systems base their security on the need of extremely powerful computers to break them down. With the promising growth of quantum computers [23], this safety seems to be put into risk in the nearest future. On the contrary, quantum cryptography protocols rely their security on the very fundamental principles of quantum mechanics [24] like the uncertainty principle or the non-cloning theorem [25]. In this section several protocols are introduced to finally motivate why Device-Independent Quantum Key Distribution represents an encouraging next-step to take in the development of safer communications.

1.2.1 Quantum Key Distribution: BB84

This protocol was proposed by Bennett and Brassard in 1984 [26], which provided it with the widely known name of BB84 protocol. Its simplicity is as remarkable as its importance in the development of quantum cryptography. It is based on the idea of the one-time pad, in which a secret key is shared between two parts. This secret key will allow them to establish a completely secure communication after it has been succesfully shared between them, thus no sensible information is sent before this point. If the protocol is unsuccesful, it will be repeated once and again until it is succesful, and then the safe communication can start. All the necessary assumptions to be made will be analysed with more detail for general Quantum Key Distribution (QKD) protocols in the next section;

Alice	Random bit	1	0	0	0	1	1	0	1	0	1	1	1
	Random basis	R	R	D	D	D	R	D	D	R	R	D	R
	Polarization	$\rightarrow$	$\uparrow$	$\nwarrow$	$\nwarrow$	$\nearrow$	$\rightarrow$	$\nwarrow$	$\nearrow$	$\uparrow$	$\rightarrow$	$\nearrow$	$\rightarrow$
Bob	Random basis	D	R	D	R	R	R	R	D	D	D	D	R
	Outcome	1	0	0	1	0	1	0	1	0	0	1	1
Check of correct basis		✗	✓	✓	✗	✗	✓	✗	✓	✗	✗	✓	✓
Check of random bits			0				1						1
Shared secret key				0					1			1	

Table 1.1: Example of the completion of BB84 protocol, from the generation of the bit string until sharing the secret key.

the purpose for the present one is, on the other hand, to introduce one of the many examples of QKD protocols in order to understand its basic principles. Following the original approach, and in line with the rest of the thesis, we will consider the encoding of the information by means of the polarization of photons. Alice will send polarized photons to Bob, with either horizontal ($|\rightarrow\rangle$), vertical ($|\uparrow\rangle$), 45º ($|\nearrow\rangle = \frac{1}{\sqrt{2}}(|\rightarrow\rangle + |\uparrow\rangle)$) or -45º ($|\nwarrow\rangle = \frac{1}{\sqrt{2}}(|\rightarrow\rangle - |\uparrow\rangle)$) polarization. Alice and Bob can choose between two different measurement basis: the rectangular basis (R) and diagonal basis (D). Note that when measuring horizontally and vertically polarized photons in the rectangular basis, it gives unequivocally whether the photon was horizontal or vertical, whereas measuring in the diagonal basis gives either result with 50% probability (and viceversa for the diagonal basis). Horizontal and 45º photons are identified with a logical value of 1. On the other hand, vertical and -45º photons are identified with the 0 logical value.

An example of the protocol is detailed in Table 1.1. Alice starts the protocol by generating two random strings, for which she needs a random number generator: one string of random bits (1 and 0) and another one with the two different basis of measurement (R and D). Then she can prepare the corresponding polarized photons: for example, to prepare a logical 1 in the diagonal basis, she will send a $|\nwarrow\rangle$ photon. Thus she sends a photon for every bit of the string to Bob. Bob, on the other hand, will also generate a random string (with his own random number generator) specifying in which basis he is going to measure every photon that he receives from Alice. In case a photon is lost in the way, that element is disregarded from the string of bits. He measures every photon's polarization that arrives succesfully according to the string of random basis he just generated. If he uses the same basis to measure the polarization of one photon as the one Alice used when generating it, then he will obtain the same logical value that she encoded; if, on the contrary, he used the other basis, there is a 50% probability that he will hit the correct logical value. After the whole string has been measured, Alice and Bob establish classical communication through an authenticated channel (this means, the communication is public but the exchanged information can not be modified by any third party). In this conversation they will compare *only* which basis they used to measure the polarization of their photons, and thus they will keep those bits that correspond to elements of the string in which they used the same basis and disregard the rest. Those bits that are kept, constitute the secret key with which they can build a safe communication.

What could a potential eavesdropper (commonly named Eve) do to steal the secret key? The most naive approach one could imagine is that she intercepts the photons that Alice sends to Bob, make a copy, and then send them to Bob so they do not notice her action. Luckily, this is not allowed by the no-cloning theorem [25], developed by Wootters and Zurek in 1982. However, Eve can still measure the photon she intercepts and generate another one that she sends to Bob. She can guess the correct basis in which she should measure with a 50% probability, which establishes a bound of 1/2 on the amount of bits that she can steal. Furthermore, there is 50% probability that the photon she intercepts is polarized in the basis that she chose, thus she will insert a 25% of error when sending the photon to Bob. In order for Alice and Bob to know if she intervened or not, they will sacrifice some of their succesful bits and compare them through the classical channel (see again Table 1.1). If the success rate is lower than the error probability induced by the eavesdropper, they have to re-start the protocol. Note that this also sets a threshold on the allowed experimental error of the protocol, which can not be higher than the one induced by Eve: else, the action of the eavesdropper could not be detected. In the next section further actions of the eavesdropper will be analysed in a broader QKD context.

1.2.2 Device-Independent Quantum Key Distribution

The connection between the violation of Bell's inequality and the safety of a cryptographic quantum protocol was proposed for the first time in the famous short publication by Eckert in 1991, which named the protocol as E91 onwards [27]. Contrary to BB84, in which Alice sent the particles to Bob, in E91 Alice and Bob receive half of an EPR pair each, which was generated by a third party. Eckert modelled the potential action of the eavesdropper by introducing elements of "*physical reality*" in the form of a certain strategic measurement, that only gives a succesful result within the constraints of Bell's inequality. Therefore, if it is violated, the eavesdropper could not have interfered with the protocol and extract information without being detected. However, the proposal did not provide with further details about the actual relization of security proofs or the experimental implementation. Also, all the measurements in which a particle is not registered are discarded in the protocol, opening the possibility for Eve to bias the detection of events. Furthermore, it was proven shortly after [28] that E91 and BB84 are security equivalent. If Alice generated the EPR pair used in E91 and, after measuring her part, she sent the other particle to Bob, we easily see that the scenario is identical to BB84[4]. They prove that the lack of success of the eavesdropper, as suggested by Eckert, is not based on the violation of the inequality but on the actual incapability of generating a state correlated with the EPR pair. She can not generate a state that can provide with information about the measurement outcomes under the rules of quantum mechanics without being noticed by Alice and Bob. It is simple to understand why: following [28], imagine that Alice and Bob share the state

$$|A, B\rangle = \left|\psi^-\right\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right) . \tag{1.12}$$

Eve can add a third-party in the state shared by Alice and Bob such that she gets information from the measurement that they perform. To do so, she should take over the generation of the pair and create a general state such as:

$$|A, B, E\rangle = \frac{1}{2}\left(|00\rangle |E_1\rangle + |01\rangle |E_2\rangle + |10\rangle |E_3\rangle + |11\rangle |E_1\rangle\right) . \tag{1.13}$$

This way, Eve only has to wait until Alice and Bob perform their measurements and measure her own part of the system. Depending on the outcome she obtains, she will know whether Alice and

[4]Despite the fact that, as Eckert argued after the publication of [28], the stored information in BB84 is classical, whereas in E91 can remain stored in the EPR pair until the key is needed and thus the action of Eve would be easily detected in the disturbance of the system.

Bob measured $|00\rangle$, $|01\rangle$, $|10\rangle$ or $|11\rangle$. However, she wants to be undetected by them. As Alice and Bob expect to share $|\psi^-\rangle$, $|A, B, E\rangle$ has to be restricted to having only -1 eigenvalues (as these are the eigenvalues of $|\psi^-\rangle$: each subsystem will have opposite eigenvalues ± 1, thus in both cases the total eigenvalue is -1) under the measurement in z and x basis. To be undetected when they measure in the z basis, the state Eve generates has to be constraint to

$$|A, B, E\rangle = \frac{1}{\sqrt{2}} \left(|01\rangle |E_2\rangle + |10\rangle |E_3\rangle \right) . \tag{1.14}$$

But, at the same time, it has to have eigenvalue -1 in the x basis, as they can also measure this way. The eigenvector with -1 eigenvalue in this basis is $\frac{1}{\sqrt{2}} (|01\rangle - |10\rangle)$, thus the only state that Eve can generate, in order to not be detected in any security test performed by Alice and Bob, is

$$|A, B, E\rangle = \frac{1}{\sqrt{2}} \left(|01\rangle - |10\rangle \right) |E_2\rangle , \tag{1.15}$$

which is uncorrelated from Eve's and Alice and Bob's outcomes. The eavesdropper can not generate a state that provides her with information without being uncovered. This invited to conclude that the use of EPR pairs and the violation of Bell's inequality was not providing with extra security to BB84. However, this simple argument does not account for more complex ways of attacking the quantum devices [29], or if Alice and Bob can not ensure that their measuring devices are completely trustful. If they can no longer know with complete certainty in which basis they measure, Eve could indeed generate a state, as the one described in equation 1.13.

Some years later a proposal about relaxing the level of trust in the quantum devices of the protocol was made by Mayers and Yao [30]. As explained, the security of BB84 relies on the fact that Alice knows whether she sent to Bob photons with either 0^o, 90^o, 45^o or -45^o polarization. They proved that Alice would not need to trust her photon source if she could use a self-checking source. This source needs to pass certain tests and satisfy a security proof, which imposes conditions on the measurements that, once again, were equivalent to violating Bell's inequality. This gave once more the intuition that it could be indeed possible to strenghten the security of cryptography by means of Bell violation. But the biggest breakthrough came with the publication by Barrett et al. in 2005 [31], where they proposed a QKD protocol proven to be secure only with the restriction of not allowing superluminal signalling. Not the assumption that, as in [28], quantum mechanics establish the bound on how much information Eve can achieve. The notion of a Device Independent QKD (DIQKD) idea is introduced.

The necessary assumptions in this context do not differ much from a general QKD protocol such BB84. From a broader perspective, Eve is only restricted by her impossibility to not use superluminal signaling, but she can break the rules of quantum mechanics [31]. Thus we will show that the main difference is that DIQKD is built upon less assumptions than QKD. Any QKD protocol requires that [1]:

- *Alice and Bob share an authenticated classical channel and a noise-free quantum channel.* In the context of cryptography, a channel can be either confidential, authenticated or secure. It is authenticated if it could be overheard but not manipulated. Alternatively the channel is confidential in case the information is impossible for anyone to overhear but, on the contrary, could be tampered by a third party, or secure, if neither overhearing or tampering are possible. Thus an authenticated classical channel shared by Alice and Bob will allow them to share which basis they used to measure their qubits ensuring that this information can not be manipulated although it is, in principle, public. A noise free quantum channel ensures that the transmitted quantum state does not suffer any alteration (that could be modelled, for example, via depolarising, erasure or amplitude damping channels).

- *No information is released to the exterior from Alice and Bob's locations.* No information can be sent by means of the measurements performed by the implied parts. The laboratories are isolated, in the sense that no eavesdropper can look ”over their shoulder”; therefore, no information can be gained by spying them, nor escapes from their locations. This also includes that no one has access to their classical memories, where they store the classical outputs of the protocols. We will see how fullfiling this assumption automatically ensures closing the locality loophole.

- *Quantum mechanics is correct*, as the protocols are based on its most fundamental principles.

- *Both have a pure random number generator*, which is essential for the choice of the measurement basis and relates to the free-will loophole.

For non-DIQKD protocols like BB84 or E91, additionally:

- *Alice and Bob must trust their respective quantum devices.* Eve has no access to the devices, and can therefore not manipulate them. In addition, there is no flaw that would make Alice and Bob doubt the choice they make for the basis of measurement. In BB84, for example, the choice of basis and the actual measurement that is carried out always match. This does not have necessarily to be true, without making this assumption.

In the Device-Independent scenario, however, this last assumption is not made as the eavesdropper has access to manipulating the measurement devices. Therefore, ones does not have to care of whether the apparatus was fabricated by suspicious entities or if it varies over time due to possible imperfections. Also, distrusting the quantum devices implies that simpler protocols like BB84 can not be considered secure anymore: Alice and Bob can not even know the dimension of the Hilbert space in which they are measuring [1]. Recalling BB84, this was precisely the way they both had to make sure Eve was not interfering. Bob and Alice compare their choice of basis for every photon and they discard those who do not match. In addition, they compare their outcomes to evaluate the error and detect the presence of Eve. If, however, they can not trust their measurement devices, this strategy fails as they can not prevent Eve from interfering in this comparisons by tampering the devices. Recall that, as Alice and Bob do not have complete confidence in the measurement they are performing, the argument from which we deduced that a state like the one depicted in equation 1.13 can not be created by the eavesdropper, does not hold anymore. In this context, the measurement devices are rather approached as black boxes with an classical inputs and outputs (the outcome of the measurement) [32, p. 307-319].

Let us suppose, in a similar way to how it was explained above, that Eve is in control of generating the entangled pairs that Alice and Bob will use to perform the protocol. She has to prepare $2n + 1$ systems: n for Alice, n for Bob and one for herself, that will provide her with the information about Alice and Bob's outcomes. Under above assumptions and following [31], it is possible to make a security proof which ensures that, by sharing a big enough number n of entangled pairs, there is an upper bound on the information that Eve can get from her measurement as long as Bell's inequality is violated. We can try to get an intuition about what is going on, without working with the security proof, by considering what happens with the conditional probabilities on the chosen basis and the actual outcomes. In the QKD context the correlation between Alice's and Bob's measurements can be considered classical. In BB84, for example, there is a probability distribution for each of them that describes how they will obtain correlated results when they measure in the same basis (let us say x or z) and totally uncorrelated when they don't. This can be provided by a classical random data generator, and then we could express the probability of observing the outcomes a and b conditioned to the measurements A and B, $P(a|A,\lambda)$ and $P(b|B,\lambda)$, in the following way, as explained in [32, p. 307-319]:

$$P(ab|AB) = \sum_{\lambda} P(\lambda) P_{\lambda}(a|A,\lambda) P_{\lambda}(b|B,\lambda)\,, \tag{1.16}$$

where $P(\lambda)$ is the probability distribution for a certain classical variable λ that correlates the outcome of the measurement with the actual chosen measurement. Therefore, if Eve has access to this variable λ when also having access to the measurement devices (as it is expected to happen in DIQKD), she can know all the outcome distributions beforehand. However, *if Bell's inequality is violated*, $P(ab|AB)$ can not be written in that form [7], precisely as proved in the section 1.1. Thus, the non-local nature of quantum mechanics allows to limit Eve's access to information, even if she has control over the generation of the pairs and access to the quantum devices.

However, the perspective of implementing DIQKD protocols experimentally looks just as exciting as demanding. As Bell's inequality has to be violated, the same experimental challenges that were explained in section 1.1.2 need to be overcome, both the locality and detections loopholes. Nevertheless, the context is different: whereas in a Bell test we intend to verify the very fundamental principles of quantum mechanics, overcoming the loopholes in the Device-Independent scenario tries to bound the advantage Eve might have by exploiting them [1]. If we recall some of the assumptions that are made in any quantum key distribution protocol we see that, in fact, the loopholes are assumed to be partially closed too. We stated that there is no subluminal signalling between Alice and Bob that could allow them to know beforehand the sets of measurements they are choosing, due to the fact that their laboratories are isolated. Furthermore, they have a (quantum) random number generator that decides the measurement sets, thus Eve has no way to anticipate their choice. Both conditions automatically close the locality loophole. Therefore the detection loophole will be the only experimental challenge to face regarding the violation of Bell's inequality and it is actually more complex in the Device-Independent scenario. As in Bell tests, the fair-sampling assumption is not possible if we want to prevent the protocol from the attacks of the eavesdropper. Eve could bias the photons that are not detected, hidden within the inefficiency of the set-up and detectors. The events in which photons are not detected can not be disregarded, regardless of whether they were lost or the detector efficiency prevented from identifying them. Thus the efficiency of detection will play an important role in overcoming of detection loophole, establishing a threshold of at least 92% required efficiency [1]. This threshold is higher than the one we pointed out for the CHSH inequality due to the additional need of performing a security proof that guarantees that the key is delivered safely. A way to work around this loophole consists in heralding the reception of the entangled pair to Alice and Bob, in a similar way to a quantum non-demolishing measurement (QND) [33]. In case both Alice and Bob receive a positive message from the heralding system, they are ready to measure the entangled photons, avoiding the detection loophole. All these technical requirements make of DIQKD a challenging experimental implementation which has still not been carried out succesfully.

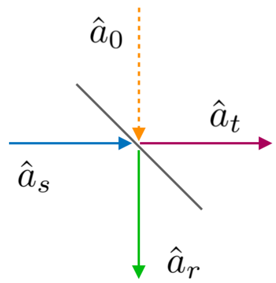

Figure 1.2: Description of the transformation that the beam splitter performs over the incoming field ($\hat{a}_s$) and the vacuum field ($\hat{a}_0$). The reflected mode is given by $\hat{a}_r$ and the transmitted one by $\hat{a}_t$.

1.3 Hong-Ou-Mandel Interference

The Hong-Ou-Mandel effect was firstly described and realised experimentally by C. K. Hong, Z. Y. Ou and L. Mandel in 1987 [34]. It was introduced in order to measure the time intervals between emitted photons by parametric down conversion. Nowadays, however, the Hong-Ou-Mandel (HOM) interference is widely used as a tool to study properties of quantum implementations (such the visibility of single-photon sources, as explained in section 3.2), as well as fundamental characteristics of quantum mechanics itself [35]. The key essence of this interference effect is manifested when two single photons interfere on a 50:50 beam splitter. To understand this effect we start by describing how a beam splitter works. A beam splitter is an optical element that consists of either birrefringent glass prisms or mirrors and have two input and two output ports. It reflects and transmits the incoming photon with a determined probability given by its transmittance (T) and reflectance (R). Therefore the state of the photon after the beam splitter is a superposition of reflected and transmitted states. Note that the quantum mechanical description of a beam splitter for a single incoming photon needs to include vacuum in one of the ports in order to satisfy the commutation relations of the photon operators. This is described by a general unitary transformation over the vacuum field and the incoming mode, $\hat{U}_{BS}$:

$$\begin{pmatrix} \hat{a}_r \\ \hat{a}_t \end{pmatrix} = \hat{U}_{BS} \begin{pmatrix} \hat{a}_0 \\ \hat{a}_s \end{pmatrix} , \tag{1.17}$$

which, following [9, p. 138], equals:

$$\begin{pmatrix} \hat{a}_r \\ \hat{a}_t \end{pmatrix} = \begin{pmatrix} t' & r \\ r' & t \end{pmatrix} \begin{pmatrix} \hat{a}_0 \\ \hat{a}_s \end{pmatrix} , \tag{1.18}$$

where the vacuum field is represented by $\hat{a}_0$, the reflected mode is given by $\hat{a}_r$ and the transmitted one by $\hat{a}_t$ (see Figure 1.2). Moreover, the following relations are satisfied:

$$|r'| = |r|, \quad |t'| = |t|, \quad |r|^2 + |t|^2 = 1, \quad r^* t' + r' t^* = 0, \quad r^* t + r' t'^* = 0 \, . \tag{1.19}$$

We next choose the above parameters in terms of the transmittance T as

$$t' = t = \sqrt{T}, \quad r' = r = i\sqrt{1-T} \, , \tag{1.20}$$

which is equivalent to setting the imaginary phase for the transmittance and reflectance to 0 and $\pi/2$ respectively. It can be verified that the transformation $\hat{U}_{BS}$ is unitary and satisfies all the

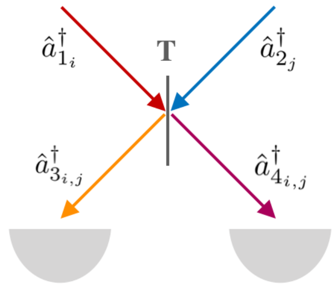

Figure 1.3: Two input photons with different modes i and j arrive to a beam splitter with transmittance T.

relations from equation 1.19. Substituting 1.20 in equation 1.18:

$$\begin{pmatrix} \hat{a}_r \\ \hat{a}_t \end{pmatrix} = \begin{pmatrix} \sqrt{T} & i\sqrt{1-T} \\ i\sqrt{1-T} & \sqrt{T} \end{pmatrix} \begin{pmatrix} \hat{a}_0 \\ \hat{a}_S \end{pmatrix} \Rightarrow \begin{pmatrix} \hat{a}_0 \\ \hat{a}_s \end{pmatrix} = \begin{pmatrix} \sqrt{T} & -i\sqrt{1-T} \\ -i\sqrt{1-T} & \sqrt{T} \end{pmatrix} \begin{pmatrix} \hat{a}_r \\ \hat{a}_t \end{pmatrix} . \tag{1.21}$$

Therefore, taking the hermitian conjugate of equation 1.21, the creation operator of the photon that arrives to the first port of the beam splitter is:

$$\hat{a}^\dagger_s = i\sqrt{1-T}\hat{a}^\dagger_r + \sqrt{T}\hat{a}^\dagger_t \tag{1.22}$$

Let us take a step forward now. Imagine that the two photons that arrive at the beam splitter have different modes i and j, that could be, for example, different temporal modes, arrival times or polarizations. For simplicity, we identify the four different beam splitter modes as 1,2,3,4. Thus, the creation operators of each of them are labeled as $\hat{a}^\dagger_{1_i}$ and $\hat{a}^\dagger_{2_j}$, respectively (see Figure 1.3). The input state that reaches the beam splitter is:

$$|\psi_{in}\rangle = |1_i, 1_j\rangle = \hat{a}^\dagger_{1_i}\hat{a}^\dagger_{2_j} |\emptyset\rangle . \tag{1.23}$$

Applying the transformation described in equation 1.21 to the creation operators, we obtain the output state:

$$\begin{aligned} |\psi_{out}\rangle &= \left(i\sqrt{1-T}\hat{a}^\dagger_{3_i} + \sqrt{T}\hat{a}^\dagger_{4_i}\right)\left(\sqrt{T}\hat{a}^\dagger_{3_j} + i\sqrt{1-T}\hat{a}^\dagger_{4_j}\right)|\emptyset\rangle \\ &= \left(i\sqrt{T(1-T)}\hat{a}^\dagger_{3_i}\hat{a}^\dagger_{3_j} - (1-T)\hat{a}^\dagger_{3_i}\hat{a}^\dagger_{4_j} + T\hat{a}^\dagger_{3_j}\hat{a}^\dagger_{4_i} + i\sqrt{T(1-T)}\hat{a}^\dagger_{4_i}\hat{a}^\dagger_{4_j}\right)|\emptyset\rangle . \end{aligned} \tag{1.24}$$

If the beam splitter is 50:50, then the output state reduces to:

$$|\psi_{out}\rangle = \frac{1}{2}\left(i\hat{a}^\dagger_{3_i}\hat{a}^\dagger_{3_j} - \hat{a}^\dagger_{3_i}\hat{a}^\dagger_{4_j} + \hat{a}^\dagger_{3_j}\hat{a}^\dagger_{4_i} + i\hat{a}^\dagger_{4_i}\hat{a}^\dagger_{4_j}\right)|\emptyset\rangle \tag{1.25}$$

Here is when all the interesting physics begin: if the two incoming photons are indistinguishable, that is, they are not in different modes ($i = j$), then the output state is a superposition state:

$$|\psi_{out}\rangle = \frac{1}{2}\left(i\hat{a}^{\dagger 2}_3 - \hat{a}^\dagger_3\hat{a}^\dagger_4 + \hat{a}^\dagger_3\hat{a}^\dagger_4 + i\hat{a}^{\dagger 2}_4\right)|\emptyset\rangle = \frac{i}{2}\left(\hat{a}^{\dagger 2}_3 + \hat{a}^{\dagger 2}_4\right)|\emptyset\rangle = \frac{i}{\sqrt{2}}\left(|2,0\rangle + |0,2\rangle\right) , \tag{1.26}$$

with both photons going together to either one detector or other, thus no coincidence clicks between both detectors are ever detected[5]. This effect is known as *bunching*. A way to understand what

[5] Note that we have taken into account that $\hat{a}^\dagger |n\rangle = \sqrt{1+n}\,|n+1\rangle$.

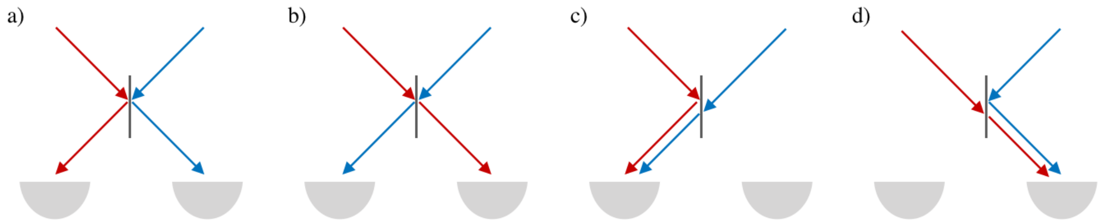

Figure 1.4: All the four different paths that lead to the interference of indistinguishable photons when interacting through a 50:50 beam splitter, creating the HOM effect. Paths a) and b) interfere destructively, whereas paths c) and d) are completely distinguishable and do not interfere, generating the bunch of the photons in the output state.

ocurres is to think of how all the possible paths that photons can take interfere. Figure 1.4 shows the four different options: either they click on different detectors or bunch and click in the same one. Due to the extra phase that it is gained with the reflection, the paths a) and b), that correspond to the terms $-\hat{a}_3^\dagger\hat{a}_4^\dagger$ and $\hat{a}_3^\dagger\hat{a}_4^\dagger$ in equation 1.26, interfere destructively. On the contrary, paths c) and d), corresponding to the terms $i\hat{a}_3^{\dagger 2}$ and $i\hat{a}_4^{\dagger 2}$, are distinguishable paths that do not interfere, thus only contributing with a global phase i to the output state. If the two input photons are not completely indistinguishable the paths a) and b) in Figure 1.4 do not interfere and thus all four different combinations of clicks on the detectors are equally probable. We can also approach the effect by calculating the coincidence probability P_{cc} using equation 1.24 for indistinguishable photons as:

$$P_{cc_{ind}} = \langle\psi_{out}|\psi_{out}\rangle_{cc} = \langle\emptyset|\left(-(1-T)\hat{a}_3\hat{a}_4 + T\hat{a}_3\hat{a}_4\right)\left(-(1-T)\hat{a}_3^\dagger\hat{a}_4^\dagger + T\hat{a}_3^\dagger\hat{a}_4^\dagger\right)|\emptyset\rangle = (2T-1)^2\ , \tag{1.27}$$

which, in fact, verifies that $P_{cc_{ind}}(T=1/2)=0$. If, on the contrary, we assign different polarizations to the incoming photons:

$$\begin{aligned} P_{cc_{dis}} = \langle\psi_{out}|\psi_{out}\rangle_{cc} &= \langle\emptyset|\left(-(1-T)\hat{a}_{3_H}\hat{a}_{4_V} + T\hat{a}_{3_V}\hat{a}_{4_H}\right)\left(-(1-T)\hat{a}_{3_H}^\dagger\hat{a}_{4_V}^\dagger + T\hat{a}_{3_V}^\dagger\hat{a}_{4_H}^\dagger\right)|\emptyset\rangle \\ &= (1-T)^2 + T^2\ , \end{aligned} \tag{1.28}$$

that gives $P_{cc_{dis}}(T=1/2)=1/2$, that is, a 50% probability of both detectors clicking simultaneously for distinguishable photons. The HOM effect is, therefore, a very useful way to determine the degree of distinguishability of two photons. In the original experiment they vary the displacement of the beam splitter towards the detectors, so that the incoming photons do not click simultaneously. Depending on the degree of displacement $c\tau$ (with τ being the time delay between the arrival of the incoming photons to the two input ports of the beam splitter), the probability of measuring coincidence counts goes from 0 for $\tau=0$ to 1 for a sufficiently big displacement compared to the inverse of the bandwidth of the photons. In reality as photons are not completely monochromatic but present a certain bandwidth $\Delta\omega$, the dip in the probability of coincidence counts becomes a function of this width [34]:

$$P_{cc} \approx 1 - e^{-(\Delta\omega\tau)^2}\ . \tag{1.29}$$

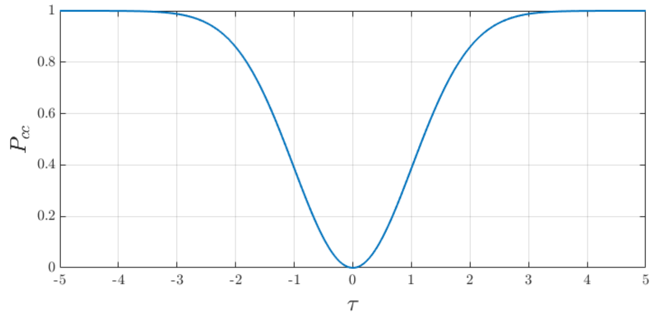

Figure 1.5: Probability of coincidence counts P_{cc} as a function of the time delay in the arrival of photons to the input ports of the beam splitter. The plot shows the so called HOM dip.

The plot of the probability of coincidence counts versus the displacement of the beam splitter exhibits the so called HOM dip (Figure 1.5). The normalized difference between the maximum and minumum of the HOM dip is defined as the visibility of the sources that generated the photons [35]:

$$V = \frac{P_{cc_{max}} - P_{cc_{min}}}{P_{cc_{max}}} \, . \tag{1.30}$$

1.4 Density matrix tomography

Throughout the thesis we will be interested in measuring a determined state of the system in the form of its density matrix *before* the measurement is carried out. For this purpose, quantum tomography provides with a process that allows to reconstruct any state by means of a certain number of measurements that depends on the size of the Hilbert space of the state. It is based on the idea that any matrix can be written in terms of a certain basis, and therefore, finding the appropiate coefficients allows to reconstruct it. Following [36] in this section, in the simplest case of a single qubit, the density matrix can be written in terms of the so called Stokes parameters S_i and the basis formed by the Pauli matrices:

$$\rho = \frac{1}{2} \sum_{i=0}^{3} S_i \hat{\sigma}_i \, , \tag{1.31}$$

where the pauli matrices are:

$$\hat{\sigma}_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \hat{\sigma}_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \hat{\sigma}_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad \hat{\sigma}_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \, , \tag{1.32}$$

and the Stokes parameters are defined by:

$$S_i \equiv \mathrm{Tr}\{\hat{\sigma}_i \rho\} \, . \tag{1.33}$$

We will use, as in the previous section, the canonical base

$$\hat{a}_H^\dagger \left|\emptyset\right\rangle \equiv \left|\rightarrow\right\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad \hat{a}_V^\dagger \left|\emptyset\right\rangle \equiv \left|\uparrow\right\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \, , \tag{1.34}$$

where the Stokes parameters can be defined in terms of the probability of measuring the system in different projective states P_i as

$$\begin{aligned} S_0 &= \langle\rightarrow|\,\rho\,|\rightarrow\rangle + \langle\uparrow|\,\rho\,|\uparrow\rangle = P_H + P_V\,, \\ S_1 &= \langle\nearrow|\,\rho\,|\nearrow\rangle - \langle\nwarrow|\,\rho\,|\nwarrow\rangle = P_D - P_A\,, \\ S_2 &= \langle\circlearrowright|\,\rho\,|\circlearrowright\rangle - \langle\circlearrowleft|\,\rho\,|\circlearrowleft\rangle = P_R - P_L\,, \\ S_3 &= \langle\rightarrow|\,\rho\,|\rightarrow\rangle - \langle\uparrow|\,\rho\,|\uparrow\rangle = P_H - P_V\,, \end{aligned} \tag{1.35}$$

where the diagonal and circular states are defined as usual:

$$\begin{aligned} |\nearrow\rangle &= \frac{1}{\sqrt{2}}\left(|\rightarrow\rangle + |\uparrow\rangle\right), \quad |\circlearrowright\rangle = \frac{1}{\sqrt{2}}\left(|\rightarrow\rangle + i\,|\uparrow\rangle\right) \\ |\nwarrow\rangle &= \frac{1}{\sqrt{2}}\left(|\rightarrow\rangle - |\uparrow\rangle\right), \quad |\circlearrowleft\rangle = \frac{1}{\sqrt{2}}\left(|\rightarrow\rangle - i\,|\uparrow\rangle\right). \end{aligned} \tag{1.36}$$

So by substituting in equation 1.31 any one-qubit density matrix can be reconstructed by measuring the state in the projective states given in equation 1.35 as:

$$\rho = \frac{1}{2}\begin{pmatrix} 2P_H & (P_D - P_A) - i\,(P_R - P_L) \\ (P_D - P_A) + i\,(P_R - P_L) & 2P_V \end{pmatrix}. \tag{1.37}$$

For the n-qubit case, the Stokes formula generalizes to:

$$\rho = \frac{1}{2^n}\sum_{i_1,i_2,\ldots i_n}^{3} S_{i_1,i_2,\ldots i_n}\hat{\sigma}_{i_1}\otimes\hat{\sigma}_{i_2}\otimes\ldots\otimes\hat{\sigma}_{i_n}\,, \tag{1.38}$$

which, for the case that will concern us (2-qubit density matrix) reduces to:

$$\rho = \frac{1}{4}\sum_{i_1,i_2}^{3} S_{i_1,i_2}\hat{\sigma}_{i_1}\otimes\hat{\sigma}_{i_2}\,, \tag{1.39}$$

with the Stokes parameters S_{i_1,i_2} defined as:

$$S_{i_1,i_2} = \mathrm{Tr}\{(\hat{\sigma}_{i_1}\otimes\hat{\sigma}_{i_2})\,\rho\}\,. \tag{1.40}$$

For instance, S_{12} would be calculated as

$$S_{12} = \mathrm{Tr}\{(\hat{\sigma}_1\otimes\hat{\sigma}_2)\,\rho\} = P_{DR} - P_{DL} - P_{AR} + P_{AL}\,, \tag{1.41}$$

Therefore, one can calculate the general 4 by 4 density matrix in terms of the Stokes parameters and then substitute them by the corresponding probabilities. Below we write explicitly all the elements of the density matrix (note that the remaining elements can be calculated by the hermitian property of the density matrix):

$$
\begin{aligned}
\rho_{11} &= P_{HH}\,, \\
\rho_{12} &= \frac{1}{2}(P_{HD} - P_{HA} - i(P_{HR} - P_{HL}))\,, \\
\rho_{13} &= \frac{1}{2}(P_{DH} - P_{AH} - i(P_{RH} - P_{LH}))\,, \\
\rho_{14} &= \frac{1}{2}(P_{DD} - P_{DA} - P_{AD} + P_{AA} - P_{RR} + P_{RL} + P_{LR} - P_{LL} + \\
&\quad - i(P_{DR} - P_{DL} - P_{AR} + P_{AL} + P_{RD} - P_{RA} - P_{LD} + P_{LA}))\,, \\
\rho_{22} &= P_{HV}\,, \\
\rho_{23} &= \frac{1}{2}(P_{DD} - P_{DA} - P_{AD} + P_{AA} + P_{RR} - P_{RL} - P_{LR} + P_{LL} + \\
&\quad - i(-P_{DR} + P_{DL} + P_{AR} - P_{AL} + P_{RD} - P_{RA} - P_{LD} + P_{LA}))\,, \\
\rho_{24} &= \frac{1}{2}(P_{DV} - P_{AV} - i(P_{RV} - P_{LV}))\,, \\
\rho_{33} &= P_{VH}\,, \\
\rho_{34} &= \frac{1}{2}(P_{VD} - P_{VA} - i(P_{VR} - P_{VL}))\,, \\
\rho_{44} &= P_{VV}\,.
\end{aligned}
\tag{1.42}
$$

Chapter 2

Implementation via single-photon sources

We have detailed in the introduction what the main experimental challenges are regarding the implementation of a DIQKD protocol. As the same time as the locality loophole can be closed by ensuring a sufficient distance between Alice and Bob in isolated stations, the detection loophole remains as the main obstacle to overcome. In this chapter we will introduce the set-up proposed by [2], which uses an heralding scheme to prevent the implementation from opening the detection loophole in relation to the transmission efficiency. Furthermore, we will analyse how the heralding procedure generates the entangled state that Alice and Bob will use to perform the protocol.

2.1 Introduction to the protocol and set-up

Despite choosing a mechanism that helps to close the loopholes, the final success of the DIQKD protocol will be proven along the thesis to be highly dependent on the quality of the single-photon sources (SPS) used to generate the transmitted photons. Therefore, the choice of which kind of source should generate the single photons is very relevant. The quality of a single-photon source is determined by several parameters: the purity of the generated photons, that measures by means of the second order correlation function $g^{(2)}$ the probability of the source to emit several photons at once (perfect purity would imply that truly single photons are being generated); the distinguishability of photons regarding their temporal pulse shape, which is measured performing HOM interference (see section 3.2) and whether photons can be generated on-demand. A very promising candidate that fullfils satisfactorily all these criteria is a single-photon source based on InGaAs quantum dots (QD) embedded in nanostructures. Contrary to photons generated by Spontaneous Parametric-Down-Conversion (SPDC) [37], quantum dot SPS can generate them deterministically, and can achieve more than 99.4% purity and a indistinguishability up to 94% [3]. Thanks to the nanostructure in which the quantum dot is embedded, one is able to couple the emmitted photon, as the direction in which the quantum dot emmits it can not be anticipated. The coupling efficiency to the nanostructure has been proven to be as high as 98% [38]. We will thus conclude that single-photons sources based on InGaAs quantum dots are a very good choice for the generation of the photons of the protocol.

The scheme suggested by [2] consists of three different parts (see Figure 2.1): Alice and Bob's

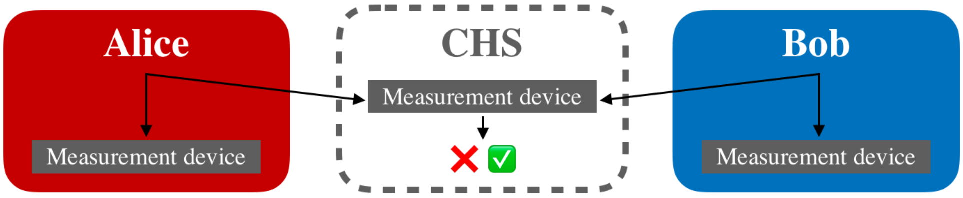

Figure 2.1: Simple scheme of the main parts of the set-up proposed by [2]. Alice and Bob each generate a pair of photons with orthogonal polarization. One from each pair is transmitted to a central heralded station (CHS), which performs a Bell state measurement on them that creates entanglement in polarization between the two photons that stayed in Alice and Bob's laboratories. The CHS will send a positive or negative message back to Alice and Bob, indicating if photons arrived succesfully (thus clossing the detection loophole) and, depending on the detection pattern, if the desired entangled state was generated.

laboratories, and a central heralding station (CHS) in between them. Each of them has a specific function and related apparatus. One can describe the functioning of the set-up as follows: Alice and Bob each generate a pair of single photons with orthogonal polarization, of which one is transmitted to the CHS and the other remains in the station where it was generated. The heralding station will perform a measurement on the two photons that it receives. This measurement, according to certain conditions that will be detailed later, will create an entangled state in polarization[1] by measurement [39] between the photons that stayed in Alice and Bob's stations. Finally, both Alice and Bob measure the state of their respective photons in a determined basis in order to proceed with the protocol. The main purpose of this scheme is to be able to avoid the detection loophole described in the Introduction by means of the heralding station: due to the fact that Alice and Bob will not consider any event that has not been approved by the CHS, the transmission efficiency between them and the heralded station becomes irrelevant. A low transmission efficiency will only force them to wait for a longer time until a succesful event happens. The station will report when it succesfully received the photons and, then, Alice and Bob can identify the event related to that pair as a succesful one. This way, the detection loophole is closed. In some way, the heralded station acts as a Quantum Non-Demolishing (QND) measurement [33], which allows to identify the state without disturbing it. The difference is, however, that the information about the state arises from the detection pattern at the heralding station. It is, precisely, the state measurement that CHS performs what will allow Alice and Bob to know, in principle, if they succeeded with the transmission and thus close the loophole but, furthermore, they will also be able to identify the state of their entangled pair of photons.

The complete scheme is introduced in more detail in Figure 2.2. Alice and Bob's stations consist on isolated laboratories that, as explained, generate the photons and measure those that are not transmited to the heralded station. They generate the pair of photons with orthogonal polarization (horizontal and vertical) by means of two quantum dot single-photon sources. This is modeled by the creation operators

$$\hat{a}^\dagger_{s_H} |\emptyset\rangle_A = |1_H\rangle_A\,, \quad \hat{a}^\dagger_{s_V} |\emptyset\rangle_A = |1_V\rangle_A\,, \tag{2.1}$$

$$\hat{b}^\dagger_{s_H} |\emptyset\rangle_B = |1_H\rangle_B\,, \quad \hat{b}^\dagger_{s_V} |\emptyset\rangle_B = |1_V\rangle_B\,, \tag{2.2}$$

where $\hat{a}^\dagger_s$ ($\hat{b}^\dagger_s$) denotes the creation of a photon by a source from Alice (Bob). Other optical

[1]The details of how this measurement is performed are explained in the following section 1.2.

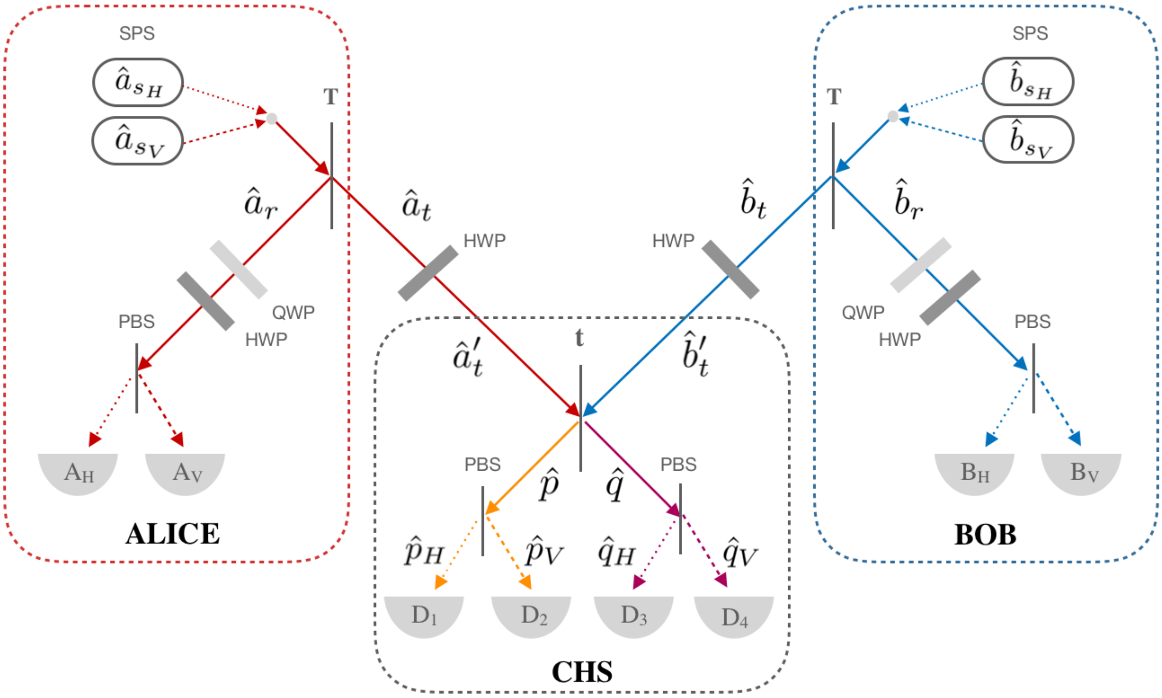

Figure 2.2: Scheme of the set-up proposed by [2], consisting on two local stations (Alice and Bob) and a central heralding station (CHS). All the different optical devices involved are indicated: beam splitters with transmittances T and t, half and quarter-waveplates (HWP and QWP), polarizing beam splitters (PBS) and single-photon sources (SPS). The photo-detectors are labeled as D_1, D_2, D_3, and D_4 for the ones belonging to the CHS and A_H (B_H) and A_V (B_V) for Alice's (Bob's) detectors, with the subindex indicating the polarization of the corresponding incoming photons. The operators that model the creation of photons at each section of the set-up are as well indicated.

devices that are part of the local stations are beam splitters (already introduced in Section 1.3) and a specific type of beam splitters: polarizing beam splitters (PBS). They have several layers of very thin dialectric material in the diagonal face that reflects and transmits the incoming beam with orthogonal polarization [40, p. 350]. In other words, depending on the polarization of the incoming photon it will be either transmitted or reflected, which is very useful in order to separate photons with different polarization that travel together in the same beam. On the other hand, the measurement devices that Alice and Bob will use consist of two different waveplates: a half-waveplate (HWP) and a quarter-waveplate (QWP). In practice, a waveplate acts as a rotation of the state in the Bloch sphere by a determined angle. The action of these two optical devices, consisting of a plate made of birrefringent material that delays the output of one polarization component of the incoming beam, is also described by unitary operations (see Section 3.2.1). The difference between a HWP and a QWP is that the delayed component falls behind either half or a quarter of the wavelength of the incoming light, respectively. In both cases, which component is delayed is determined by the angle that the device has been rotated, making them very useful in order to choose how to project the state. Finally, the detection of photons is made by measuring the electric field, usually, by photo-ionization: the detectors absorb one or more photons that provoque the excitation and release of an electron from a bound to a free state [41]. This process can be simplified and described with the measurement of the incoming electric field (see Section 3.2.2). In the following section we will describe more explicitly the action of all these optical devices on the photons and how entanglement is generated.

2.2 Transformation of the initial creation operators

In this section we will analyze in detail how every optical element acts on the generated photons. However, let us first have an intuitive approach on how the set-up works before describing the transformation of the creation operators. We start by considering the case in which the two photons that are transmitted from Alice and Bob's laboratories have the same polarization, and thus also the ones that stay in the local stations. The transmitted photons will arrive to the central beam splitter with either diagonal or antidiagonal polarization after the action of the HWP (the transformation will soon be detailed). If we consider, to simplify the example, that the transmittance of the

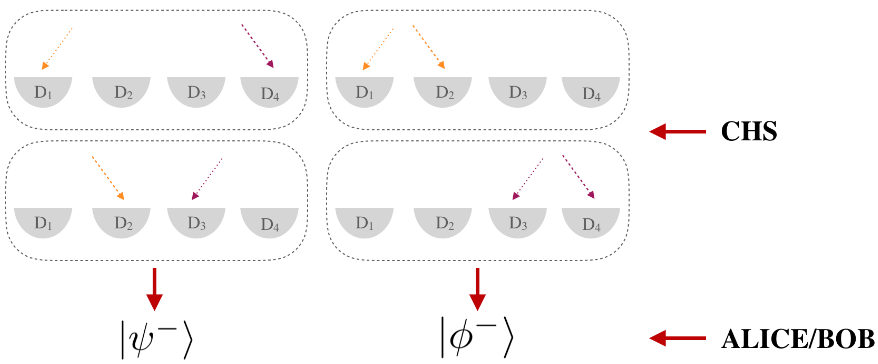

Figure 2.3: Scheme showing the dettection pattern that indicates which entangled state has been generated between Alice and Bob's photons. The central beam splitter has been set to $t = 1/2$.

beam splitter is $t = 1/2$, the photons will bunch due to their indistinguishability (see section 1.3). Therefore the detection pattern in the heralded station will consist of combinations of two clicks in detectors that correspond to the same PBS (either clicks in D_1 and D_2, or in D_3 and D_4). On the other hand, if the transmitted photons have different polarization, the beam splitter will receive a pair of distinguishable diagonal-antidiagonal photons in its input ports. No bunching will occur, thus the detection pattern in the heralded station can not only constist of clicks on D_1 and D_2, or in D_3 and D_4, but also in detectors that correspond to different PBS (clicks in D_1 and D_4, or in D_2 and D_3). On the other hand, we must take into account that, as it will be proven later, entanglement will only be generated if the detected photons have orthogonal polarization. This restricts the possible positive detection patterns to D_1D_2, D_3D_4, D_1D_4 and D_2D_3. The combinations D_1D_2 and D_3D_4 will happen only if the photons that stayed in the local stations have equal polarization, as we just explained. Given that the pattern is detected we can not know for certain the original state of the photons, the state of the pair that Alice and Bob share is, not surprisingly, proportional to $|\phi^-\rangle = \frac{1}{\sqrt{2}}\left(\hat{a}^\dagger_H\hat{b}^\dagger_H - \hat{a}^\dagger_V\hat{b}^\dagger_V\right)|\emptyset\rangle$. Moreover, the combinations D_1D_4 and D_2D_3 will occur if the photons that stayed in the local stations have different polarization, heralding that the state that Alice and Bob share must be proportional to $|\psi^-\rangle = \frac{1}{\sqrt{2}}\left(\hat{a}^\dagger_H\hat{b}^\dagger_V - \hat{a}^\dagger_V\hat{b}^\dagger_H\right)|\emptyset\rangle$ (see Figure 2.3). The combinations that generate entanglement (D_1D_2, D_3D_4, D_1D_4 and D_2D_3) represent a 50% of the total number of detection patterns that can occur, that also include those which generate separable states in Alice and Bob's photons (D_1^2, D_2^2, D_3^2 and D_4^2). This agrees with the fact that any linear-optical circuit that performs Bell-state measurement can only generate distinguishable entangled states with 50% probability [42].

Once we can intuitively understand how the heralding process works, we proceed to analize the functioning of the set-up and construct step by step the state that Alice and Bob share at the end of the process. The state of each pair of photons after their creation in each laboratory is described by

$$\hat{a}^\dagger_{s_H}\hat{a}^\dagger_{s_V}|\emptyset\rangle_A = |1_H\rangle|1_V\rangle_A\,, \quad \hat{b}^\dagger_{s_H}\hat{b}^\dagger_{s_V}|\emptyset\rangle_B = |1_H\rangle|1_V\rangle_B\ . \tag{2.3}$$

Note that, then, the global state of the system of the four photons is simply the product state

$$|1_H\rangle|1_V\rangle_A \otimes |1_H\rangle|1_V\rangle_B = \hat{a}^\dagger_{s_H}\hat{a}^\dagger_{s_V}\hat{b}^\dagger_{s_H}\hat{b}^\dagger_{s_V}|\emptyset\rangle\ . \tag{2.4}$$

After being generated, the two pairs of photons with orthogonal polarization will encounter a beam splitter with transmittance T (this transmittance is considered to be equal for both Alice and Bob's stations). In order to simpify the notation, we will denote the reflected photon as $\hat{a}^\dagger_r \equiv a^\dagger$. Applying the result obtained in equation 1.22 and including the polarization of the photon, the emmitted photons are transformed as:

$$\hat{a}^\dagger_{s_H} = i\sqrt{1-T}\hat{a}^\dagger_H + \sqrt{T}\hat{a}^\dagger_{t_H}, \quad \hat{a}^\dagger_{s_V} = i\sqrt{1-T}\hat{a}^\dagger_V + \sqrt{T}\hat{a}^\dagger_{t_V}\,, \tag{2.5}$$

and similarly for Bob's photons. The following step is to calculate the next transformations for the transmitted photons. As can be seen in Figure 2.2, these photons then go through from both Alice and Bob's sides a half-waveplate. A HWP follows the unitary transformation $\hat{U}_{HWP}(\phi)$, which is one of the so called Jones matrices [43]:

$$\hat{U}_{HWP}(\phi) = \begin{pmatrix} \cos(2\phi) & -\sin(2\phi) \\ -\sin(2\phi) & -\cos(2\phi) \end{pmatrix}\ . \tag{2.6}$$

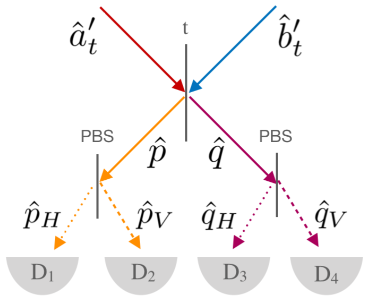

Figure 2.4: Description of the transformation that the central beam splitter of the set-up performs over the transmitted photons from Alice and Bob's stations that arrived succesfully to the CHS (given by $\hat{a}_t'$ and $\hat{b}_t'$, respectively). The outgoing beams are given by the operators $\hat{p}$ and $\hat{q}$, which encounter a polarizing beam splitter, dividing the beams depending on the polarization of the photon ($\hat{p}_H$ and $\hat{p}_V$, and $\hat{q}_H$ and $\hat{q}_V$). The final beams arrive to four photodetectors.

Therefore, by fixing the angle $\phi = -\pi/8$ for both HWP:

$$\begin{pmatrix} \hat{a}_{t_H} \\ \hat{a}_{t_V} \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} \hat{a}'_{t_H} \\ \hat{a}'_{t_V} \end{pmatrix} . \tag{2.7}$$

Thus, applying the transformation to the initial creation operators from the sources (equation 2.5):

$$\hat{a}^\dagger_{s_H} = i\sqrt{1-T}\hat{a}^\dagger_H + \sqrt{\frac{T}{2}}(\hat{a}'^\dagger_{t_H} + \hat{a}'^\dagger_{t_V}), \quad \hat{a}^\dagger_{s_V} = i\sqrt{1-T}\hat{a}'^\dagger_V + \sqrt{\frac{T}{2}}(\hat{a}'^\dagger_{t_H} - \hat{a}'^\dagger_{t_V}) . \tag{2.8}$$

Although losses are incorporated in the model thoroughly in Chapter 3, in order to follow the first approach introduced in [2], we will consider a possible loss in transmission between Alice, Bob and the heralded station. The probability of successful transmission is given by η_t, so therefore:

$$\hat{a}^\dagger_{s_H} = i\sqrt{1-T}\hat{a}^\dagger_H + \sqrt{\frac{\eta_t T}{2}}(\hat{a}'^\dagger_{t_H} + \hat{a}'^\dagger_{t_V}), \quad \hat{a}^\dagger_{s_V} = i\sqrt{1-T}\hat{a}^\dagger_V + \sqrt{\frac{\eta_t T}{2}}(\hat{a}'^\dagger_{t_H} - \hat{a}'^\dagger_{t_V}) . \tag{2.9}$$

Once the photons reach the heralded station they encounter another beam splitter, this time with transmittance t (see Figure 2.4). Following 1.21:

$$\begin{pmatrix} \hat{b}_t' \\ \hat{a}_t' \end{pmatrix} = \begin{pmatrix} \sqrt{t} & -i\sqrt{1-t} \\ -i\sqrt{1-t} & \sqrt{t} \end{pmatrix} \begin{pmatrix} \hat{p} \\ \hat{q} \end{pmatrix} . \tag{2.10}$$

Thus, equation 2.9 is transformed by 2.10 as:

$$\hat{a}^\dagger_{s_H} = i\sqrt{1-T}\hat{a}^\dagger_H + \sqrt{\frac{\eta_t T}{2}}(i\sqrt{1-t}\hat{p}^\dagger_H + \sqrt{t}\hat{q}^\dagger_H + i\sqrt{1-t}\hat{p}^\dagger_V + \sqrt{t}\hat{q}^\dagger_V), \tag{2.11}$$

$$\hat{a}^\dagger_{s_V} = i\sqrt{1-T}\hat{a}^\dagger_V + \sqrt{\frac{\eta_t T}{2}}(i\sqrt{1-t}\hat{p}^\dagger_H + \sqrt{t}\hat{q}^\dagger_H - (i\sqrt{1-t}\hat{p}^\dagger_V + \sqrt{t}\hat{q}^\dagger_V)) . \tag{2.12}$$

Note that this beam splitter is the one that weights the mix of photons coming from Alice and Bob, depending on the value of t. This means, that it is expected that t will govern the level of entanglement of the remaining pair after the measurement of the CH station. Re-organising the terms and applying the same transformations on Bob's pair of generated photons, we obtain:

$$\begin{aligned}
\hat{a}^\dagger_{s_H} &= \sqrt{\frac{\eta_t T}{2}}(i\sqrt{1-t}(\hat{p}^\dagger_H + \hat{p}^\dagger_V) + \sqrt{t}(\hat{q}^\dagger_H + \hat{q}^\dagger_V)) + i\sqrt{1-T}\hat{a}^\dagger_H,\\
\hat{a}^\dagger_{s_V} &= \sqrt{\frac{\eta_t T}{2}}(i\sqrt{1-t}(\hat{p}^\dagger_H - \hat{p}^\dagger_V) + \sqrt{t}(\hat{q}^\dagger_H - \hat{q}^\dagger_V)) + i\sqrt{1-T}\hat{a}^\dagger_V,\\
\hat{b}^\dagger_{s_H} &= \sqrt{\frac{\eta_t T}{2}}(\sqrt{t}(\hat{p}^\dagger_H + \hat{p}^\dagger_V) + i\sqrt{1-t}(\hat{q}^\dagger_H + \hat{q}^\dagger_V)) + i\sqrt{1-T}\hat{b}^\dagger_H,\\
\hat{b}^\dagger_{s_V} &= \sqrt{\frac{\eta_t T}{2}}(\sqrt{t}(\hat{p}^\dagger_H - \hat{p}^\dagger_V) + i\sqrt{1-t}(\hat{q}^\dagger_H - \hat{q}^\dagger_V)) + i\sqrt{1-T}\hat{b}^\dagger_V\,.
\end{aligned} \tag{2.13}$$

Thus, the total transformation for each pair generated with orthogonal polarization in Alice and Bob's labs is:

$$\begin{aligned}
&\hat{a}^\dagger_{s_H}\hat{a}^\dagger_{s_V} = \frac{\eta_t T}{2}\left[-(1-t)(\hat{p}^{\dagger 2}_H - \hat{p}^{\dagger 2}_V) + t(\hat{q}^{\dagger 2}_H - \hat{q}^{\dagger 2}_V) + 2i\sqrt{t(1-t)}(\hat{p}^\dagger_H\hat{q}^\dagger_H - \hat{p}^\dagger_V\hat{q}^\dagger_V)\right]\\
&+ i\sqrt{\frac{\eta_t T(1-T)}{2}}\left[\hat{a}^\dagger_H(i\sqrt{1-t}(\hat{p}^\dagger_H - \hat{p}^\dagger_V) + \sqrt{t}(\hat{q}^\dagger_H - \hat{q}^\dagger_V)) + \hat{a}^\dagger_V(i\sqrt{1-t}(\hat{p}^\dagger_H + \hat{p}^\dagger_V) + \sqrt{t}(\hat{q}^\dagger_H + \hat{q}^\dagger_V))\right]\\
&- (1-T)\hat{a}^\dagger_H\hat{a}^\dagger_V,\\[2ex]
&\hat{b}^\dagger_{s_H}\hat{b}^\dagger_{s_V} = \frac{\eta_t T}{2}\left[t(\hat{p}^{\dagger 2}_H - \hat{p}^{\dagger 2}_V) - (1-t)(\hat{q}^{\dagger 2}_H - \hat{q}^{\dagger 2}_V) + 2i\sqrt{t(1-t)}(\hat{p}^\dagger_H\hat{q}^\dagger_H - \hat{p}^\dagger_V\hat{q}^\dagger_V)\right]\\
&+ i\sqrt{\frac{\eta_t T(1-T)}{2}}\left[\hat{b}^\dagger_H(\sqrt{t}(\hat{p}^\dagger_H - \hat{p}^\dagger_V) + i\sqrt{1-t}(\hat{q}^\dagger_H - \hat{q}^\dagger_V)) + \hat{b}^\dagger_V(\sqrt{t}(\hat{p}^\dagger_H + \hat{p}^\dagger_V) + i\sqrt{1-t}(\hat{q}^\dagger_H + \hat{q}^\dagger_V))\right]\\
&- (1-T)\hat{b}^\dagger_H\hat{b}^\dagger_V\,,
\end{aligned} \tag{2.14}$$

which represents all the possible situations in which the two photons can end up. The first line of each transformation compends both photons being transmitted and arriving to the heralded station. Due to bunching effects at the HWP because of the indistinguishability of photons, note that in fact there would be only simultaneous clicks with the same polarization in case both photons are transmitted from the same side ($\hat{p}^{\dagger 2}_H$, $\hat{p}^{\dagger 2}_V$, $\hat{q}^{\dagger 2}_H$, $\hat{q}^{\dagger 2}_V$, $\hat{p}^\dagger_H\hat{q}^\dagger_H$ and $\hat{p}^\dagger_V\hat{q}^\dagger_V$). These events correspond to single clicks on all detectors (given that the photo-detectors can not distinguish how many photons arrived simultaneously) and the combinations D_1D_3 and D_2D_4. The second line of the transformation describes one photon staying in the station where it was created and the other one being succesfully received at the CH station. These are the events we consider as successful because, recalling the purpose of the set-up, we want Alice and Bob to share an entangled pair that they know has the correct state thanks to the measurement performed by the CHS on the other two generated photons. This is only possible in the scenario described by the combinations of operators multiplied by the coefficient $i\sqrt{\frac{\eta_t T(1-T)}{2}}$. Finally, the terms $\hat{a}^\dagger_H\hat{a}^\dagger_V$ and $\hat{b}^\dagger_H\hat{b}^\dagger_V$ correspond to the pair staying in its respective lab without being transmitted at all, which is of course not a sucessful event.

2.3 Postselection of events at the heralded station

We are only interested in the transformation leading to succesful events, as they are the ones we will select when performing the experiment. Thus, the transformation for the whole system, selecting the terms multiplied by $i\sqrt{\frac{\eta_t T(1-T)}{2}}$ in equation 2.14, is:

$$\begin{aligned}\hat{a}^\dagger_{s_H}\hat{a}^\dagger_{s_V}\hat{b}^\dagger_{s_H}\hat{b}^\dagger_{s_V} = -\frac{\eta_t T(1-T)}{2}\cdot \\ &\Big[\hat{a}^\dagger_H(i\sqrt{1-t}(\hat{p}^\dagger_H-\hat{p}^\dagger_V)+\sqrt{t}(\hat{q}^\dagger_H-\hat{q}^\dagger_V))+\hat{a}^\dagger_V(i\sqrt{1-t}(\hat{p}^\dagger_H+\hat{p}^\dagger_V)+\sqrt{t}(\hat{q}^\dagger_H+\hat{q}^\dagger_V))\Big]\cdot \\ &\Big[\hat{b}^\dagger_H(\sqrt{t}(\hat{p}^\dagger_H-\hat{p}^\dagger_V)+i\sqrt{1-t}(\hat{q}^\dagger_H-\hat{q}^\dagger_V))+\hat{b}^\dagger_V(\sqrt{t}(\hat{p}^\dagger_H+\hat{p}^\dagger_V)+i\sqrt{1-t}(\hat{q}^\dagger_H+\hat{q}^\dagger_V))\Big]\,.\end{aligned} \tag{2.15}$$

We can construct the density matrix ρ_{tot} of the state of the photons that stayed in Alice and Bob's stations by tracing out the CHS operators $\hat{p}^\dagger_H$, $\hat{p}^\dagger_V$, $\hat{q}^\dagger_H$ and $\hat{q}^\dagger_V$ as:

$$\rho_{tot} = \mathrm{Tr}_{CHS}\left\{\hat{a}^\dagger_{s_H}\hat{a}^\dagger_{s_V}\hat{b}^\dagger_{s_H}\hat{b}^\dagger_{s_V}\left|\emptyset\right\rangle\left\langle\emptyset\right|\hat{a}_{s_H}\hat{a}_{s_V}\hat{b}_{s_H}\hat{b}_{s_V}\right\}\,, \tag{2.16}$$

where the density matrix is written in the $\left\{\hat{a}^\dagger_H\hat{b}^\dagger_H\left|\emptyset\right\rangle, \hat{a}^\dagger_H\hat{b}^\dagger_V\left|\emptyset\right\rangle, \hat{a}^\dagger_V\hat{b}^\dagger_H\left|\emptyset\right\rangle, \hat{a}^\dagger_V\hat{b}^\dagger_V\left|\emptyset\right\rangle\right\}$ basis. The subindex *tot* of ρ_{tot} stands for the fact that we are including all the combinations of clicks of the two photons arriving to the heralding station. Using the transformation from the previous equation, 2.15:

$$\begin{aligned}\rho_{tot} = \frac{\eta_t^2 T^2(1-T)^2}{2}\cdot \\ \begin{pmatrix} 2(1-2t)^2+8t(1-t) & 0 & 0 & 0 \\ 0 & (1-2t)^2+4t(1-t)+1 & (1-2t)^2+4t(1-t)-1 & 0 \\ 0 & (1-2t)^2+4t(1-t)-1 & (1-2t)^2+4t(1-t)+1 & 0 \\ 0 & 0 & 0 & 2(1-2t)^2+8t(1-t)\end{pmatrix}.\end{aligned} \tag{2.17}$$

We stress that in evaluating the above expression we considered all the possible events that can lead to two photons clicking in the heralding station. Thus, the trace of ρ_{tot} should correspond to the probability of two photons arriving succesfully to the CHS. In fact:

$$\mathrm{Tr}\{\rho_{tot}\} = \frac{\eta_t^2 T^2(1-T)^2}{2}\left(6(1-2t)^2+24t(1-t)+2\right) = 4\eta_t^2 T^2(1-T)^2\,. \tag{2.18}$$

Indeed, the probability for a successful photon to reach the heralding station is $\eta_t^2 T^2(1-T)^2$. The factor of 4 is due to the fact that there are four different combinations of generated pairs that can arrive to the CHS: both horizontal generated photons, both vertical or with orthogonal polarization. The state depicted by ρ_{tot} is not useful for the protocol: it does not correspond with any entangled state of Alice and Bob's remaining photons, nor tunable enough in t. Instead, if we select only some of the events ocurring at the heralding station, we can generate entangled states of photons in polarization when the photons that click in the middle have orthogonal polarization. With this aim, we restrict the transformation of equation 2.15 to events consisting of the arrival of photons with orthogonal polarization represented by the combinations of simultaneous clicks on detectors D_1D_2, D_3D_4, D_1D_4, and D_2D_3. Rearranging the terms we get:

$$\begin{aligned}\hat{a}^\dagger_{s_H}\hat{a}^\dagger_{s_V}\hat{b}^\dagger_{s_H}\hat{b}^\dagger_{s_V} = -\frac{\eta_t T(1-T)}{2}(&\hat{a}^\dagger_H\hat{b}^\dagger_H\left[(1-2t)(\hat{p}^\dagger_H\hat{q}^\dagger_V+\hat{p}^\dagger_V\hat{q}^\dagger_H)-2i\sqrt{t(1-t)}(\hat{p}^\dagger_H\hat{p}^\dagger_V+\hat{q}^\dagger_V\hat{q}^\dagger_H)\right]\\ &+\hat{a}^\dagger_H\hat{b}^\dagger_V\left[-(\hat{p}^\dagger_H\hat{q}^\dagger_V-\hat{p}^\dagger_V\hat{q}^\dagger_H)\right]+\hat{a}^\dagger_V\hat{b}^\dagger_H\left[(\hat{p}^\dagger_H\hat{q}^\dagger_V-\hat{p}^\dagger_V\hat{q}^\dagger_H)\right]\\ &+\hat{a}^\dagger_V\hat{b}^\dagger_V\left[-(1-2t)(\hat{p}^\dagger_H\hat{q}^\dagger_V+\hat{p}^\dagger_V\hat{q}^\dagger_H)+2i\sqrt{t(1-t)}(\hat{p}^\dagger_H\hat{p}^\dagger_V+\hat{q}^\dagger_V\hat{q}^\dagger_H)\right]).\end{aligned} \tag{2.19}$$

Following again a technique of tracing out the detection in the CHS, like in equation 2.16, it leads to the density matrix $\rho_{12,34,14,23}$:

$$\rho_{12,34,14,23} = \frac{\eta_t^2T^2(1-T)^2}{2}\begin{pmatrix}1&0&0&-1\\0&1&-1&0\\0&-1&1&0\\-1&0&0&1\end{pmatrix} = \eta_t^2T^2(1-T)^2\left(|\psi^-\rangle\langle\psi^-|+|\phi^-\rangle\langle\phi^-|\right), \tag{2.20}$$

where $|\psi^-\rangle = \frac{1}{\sqrt{2}}(\hat{a}^\dagger_H\hat{b}^\dagger_V-\hat{a}^\dagger_V\hat{b}^\dagger_H)|\emptyset\rangle$ and $|\phi^-\rangle = \frac{1}{\sqrt{2}}(\hat{a}^\dagger_H\hat{b}^\dagger_H-\hat{a}^\dagger_V\hat{b}^\dagger_V)|\emptyset\rangle$ are the previously defined Bell states. Due to the fact that we have dropped half of the events which involve two photons arriving succesfully to the CHS (we have not considered two photons arriving to the same detector, nor D_1D_3 or D_2D_4 either as they accord with same polarization photons), now the trace of the density matrix has been reduced by a factor of 2. Indeed, the probability of half of the events to happen is $2\eta_t^2T^2(1-T)^2$. Still, this state is not really useful for the protocol either, as it is a mixed state and, furthermore, it is independent of t. We seek a state whose level of entanglement can be modified by a parameter (in our case, the probability of transmission of the central beam splitter). Hence, we restrict further our analysis to events which are succesful for the protocol. For this purpose we need the photons arriving to the CHS not only to have orthogonal polarization, but also get to different polarizing beam splitters. As a result, only the detection on D_1D_4 and D_2D_3 is now considered as the correct detection event at the heralded station. Thus the transformation is reduced to:

$$\begin{aligned}\hat{a}^\dagger_{s_H}\hat{a}^\dagger_{s_V}\hat{b}^\dagger_{s_H}\hat{b}^\dagger_{s_V} = -\frac{\eta_t T(1-T)}{2}(&\hat{a}^\dagger_H\hat{b}^\dagger_H\left[(1-2t)(\hat{p}^\dagger_H\hat{q}^\dagger_V+\hat{p}^\dagger_V\hat{q}^\dagger_H)\right]+\hat{a}^\dagger_V\hat{b}^\dagger_V\left[-(1-2t)(\hat{p}^\dagger_H\hat{q}^\dagger_V+\hat{p}^\dagger_V\hat{q}^\dagger_H)\right]\\ &+\hat{a}^\dagger_H\hat{b}^\dagger_V\left[-(\hat{p}^\dagger_H\hat{q}^\dagger_V-\hat{p}^\dagger_V\hat{q}^\dagger_H)\right]+\hat{a}^\dagger_V\hat{b}^\dagger_V\left[(\hat{p}^\dagger_H\hat{q}^\dagger_V-\hat{p}^\dagger_V\hat{q}^\dagger_H)\right]).\end{aligned} \tag{2.21}$$

Tracing out again the operators $\hat{p}$ and $\hat{q}$ we obtain the density matrix $\rho_{14,23}$:

$$\rho_{14,23} = \frac{\eta_t^2T^2(1-T)^2}{2}\begin{pmatrix}(1-2t)^2&0&0&(1-2t)^2\\0&1&-1&0\\0&-1&1&0\\(1-2t)^2&0&0&(1-2t)^2\end{pmatrix}. \tag{2.22}$$

This density matrix averages the states $|\psi_{14}\rangle$ and $|\psi_{23}\rangle$, corresponding to the combination of simultaneous clicks on the detectors D_1D_4 and D_2D_3 that we restricted ourselves to (operators

$\hat{p}_H^\dagger \hat{q}_V^\dagger$ and $\hat{p}_V^\dagger \hat{q}_H^\dagger$ in equation 2.21, respectively):

$$\begin{aligned} |\psi_{14}\rangle &= -\frac{\eta_t T(1-T)}{\sqrt{2}} \left(-\left|\psi^-\right\rangle + (1-2t)\left|\phi^-\right\rangle\right), \\ |\psi_{23}\rangle &= -\frac{\eta_t^2 T^2 (1-T)^2}{\sqrt{2}} \left(\left|\psi^-\right\rangle + (1-2t)\left|\phi^-\right\rangle\right). \end{aligned} \tag{2.23}$$

In contrast with the previous density matrices, $\rho_{14,23}$ allows to tune the amount of entanglement of the state shared by Alice and Bob's photons by choosing t. The states $|\psi_{14}\rangle$ and $|\psi_{23}\rangle$ are a superposition of Bell states; if the central beam splitter is chosen to be 50:50 ($t = 0.5$), then Alice and Bob share the maximally entangled state that we predicted by argumentation in the begining of the section. On the contrary, in the limit where the central beam splitter reflects or transmits with total probability the incoming photons ($t = 0, 1$), there is no entanglement between the photons in A and B, which is why one ends up in the same mixed state as $\rho_{12,34,14,23}$. As it was mentioned in the Introduction, this ability to tuning entanglement is crucial in order to find a lower threshold of success of the protocol regarding local efficiency of the set-up by exploring other inequalities than CHSH [18].

For completeness, we finally calculate the state that would correspond to the events D_1D_2 and D_3D_4, this is, from the transformation:

$$\begin{aligned} \hat{a}_{s_H}^\dagger \hat{a}_{s_V}^\dagger \hat{b}_{s_H}^\dagger \hat{b}_{s_V}^\dagger = -\frac{\eta_t T(1-T)}{2} (&\hat{a}_H^\dagger \hat{b}_H^\dagger \left[-2i\sqrt{t(1-t)}(\hat{p}_H^\dagger \hat{p}_V^\dagger + \hat{q}_V^\dagger \hat{q}_H^\dagger)\right] \\ &+ \hat{a}_V^\dagger \hat{b}_V^\dagger \left[2i\sqrt{t(1-t)}(\hat{p}_H^\dagger \hat{p}_V^\dagger + \hat{q}_V^\dagger \hat{q}_H^\dagger)\right]), \end{aligned} \tag{2.24}$$

leading to the same state for both combinations of clicks:

$$|\psi_{12}\rangle = |\psi_{34}\rangle = 2i\eta_t T(1-T)\sqrt{t(1-t)}\left|\phi^-\right\rangle, \tag{2.25}$$

and the density matrix $\rho_{12,34}$:

$$\rho_{12,34} = 2\eta_t^2 T^2 (1-T)^2 t(1-t) \begin{pmatrix} 1 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ -1 & 0 & 0 & 1 \end{pmatrix}. \tag{2.26}$$

As a sanity check, it can be easily prove that $\rho_{14,23}$ and $\rho_{12,34}$ indeed satisfies $\rho_{14,23} + \rho_{12,34} = \rho_{12,34,14,23}$. Following the arguments presented before, this pure state is as good as $\rho_{14,23}$ regarding the entanglement generated, but the transmittance t can not modify it.

2.4 Summary

We have argued how the heralding station allows to closing the detection loophole opened by the inefficiency in transmission. Furthermore, we have argued why a post-selection of events at the heralded station leads to ensuring that Alice and Bob share the optimal state for the protocol. These combinations have been proven to be simultaneous clicks on the detectors D_1D_4 and D_2D_3, this means, photons arriving with orthogonal polarization to different polarizing beam splitters (see Figure 2.4). By making this choice, the pair of photons that stay at Alice and Bob's stations respectively share the following states, depending on the ocurred combination:

$$
\begin{aligned}
|\psi_{14}\rangle &= -\frac{\eta_t T(1-T)}{\sqrt{2}}\left(-\left|\psi^-\right\rangle + (1-2t)\left|\phi^-\right\rangle\right) \ , \\
|\psi_{23}\rangle &= -\frac{\eta_t^2 T^2 (1-T)^2}{\sqrt{2}}\left(\left|\psi^-\right\rangle + (1-2t)\left|\phi^-\right\rangle\right) \ .
\end{aligned}
\tag{2.27}
$$

The amplitudes of these entangled states depend on the transmittance t of the central beam splitter. In the following chapters, thus, we choose $D_1 D_4$ and $D_2 D_3$ to be the only events that lead to a positive message from the heralded station.

Chapter 3

Description of errors in the experiment

So far, we have assumed that the photons emitted by the sources are indistinguishable beyond their polarization [2]. This does not have to be necessarily true. Each of the sources can add noise on top of the single photon wavepacket, making it clearly distinguishable from the others and therefore affecting their final interference. Furthermore, photons can get lost at any point during the experiment, which has not yet been taken into consideration. The objective of this chapter is to describe how all these errors are modeled so the following chapters can calculate quantitatively their effect and how they can potentially influence the success of the protocol.

3.1 Time dependent operators

For completeness and in order to proceed with clarity in the following sections, we take a small step back before introducing any time dependence in the creation operators. The operators satisfy the commutation relations [9, p. 138]:

$$\left[\hat{a}_i, \hat{a}_j^\dagger\right] = \hat{a}_i\hat{a}_j^\dagger - \hat{a}_j^\dagger\hat{a}_i = \delta_{ij}, \quad [\hat{a}_i, \hat{a}_j] = \left[\hat{a}_i^\dagger, \hat{a}_j^\dagger\right] = 0\,, \tag{3.1}$$

where the index i, j stands for a particular mode and δ_{ij} is a Kronecker delta. Thus, given that $\left\langle \hat{a}_i\hat{a}_j^\dagger \right\rangle = \delta_{ij}$, a matrix element corresponding with the creation of two photons of modes i, j yields

$$\left\langle \hat{a}_i\hat{a}_j\hat{a}_i^\dagger\hat{a}_j^\dagger \right\rangle = \left\langle \hat{a}_i(\delta_{ij} + \hat{a}_i^\dagger\hat{a}_j)\hat{a}_j^\dagger \right\rangle = \delta_{ij}\left\langle \hat{a}_i\hat{a}_j^\dagger \right\rangle + \left\langle \hat{a}_i\hat{a}_i^\dagger \right\rangle \left\langle \hat{a}_j\hat{a}_j^\dagger \right\rangle = \delta_{ij} + 1\,. \tag{3.2}$$

In fact, equation 3.2 was implicitly used already in the previous chapter, when calculating matrix elements such as $\left\langle \hat{p}_H\hat{p}_V\hat{p}_H^\dagger\hat{p}_V^\dagger \right\rangle = 1$ or $\left\langle \hat{q}_H^2\hat{q}_H^{\dagger 2} \right\rangle = 2$. However, taking into account the distinguishability of photons will modify this result. The commutation relations for time dependent operators corresponding to different temporal modes:

$$\left[\hat{a}(t), \hat{a}^\dagger(t')\right] = \hat{a}(t)\hat{a}^\dagger(t') - \hat{a}^\dagger(t')\hat{a}(t) = \delta(t-t'), \quad [\hat{a}(t), \hat{a}(t')] = \left[\hat{a}^\dagger(t), \hat{a}^\dagger(t')\right] = 0\,, \tag{3.3}$$

where $\delta(t-t')$ is not a Kronecker delta anymore, but a Dirac delta. We next introduce the function $f_i(t)$, with $i = 1, 2, 3, 4$ (different for every source in which the photons are generated), such that the mode operators can be defined as

$$\hat{a}_{f_i}(t) = \int_{-\infty}^{\infty} f_i(t)\hat{a}(t)dt\,. \tag{3.4}$$

In order to simplify the notation, we denote $\hat{a}_{f_i}(t) \equiv \hat{a}_{f_i}$. The function $f_i(t)$ convolutes with each photon's creation operator differently in time. Thus, we are in fact introducing different temporal modes for each photon. In another way, the original $\hat{a}_s$ that we worked with in the previous chapter represents the creation of the wavefunction correspondent to one of the four sources. It is very likely to be identical for all of them. On the contrary, $\hat{a}_{f_i}$ takes into account the noise added to each wavepacket, different for every source and dependent of time. The above introduced functions satisfy the normalization $\int_{-\infty}^{\infty}|f_i(t)|^2dt = 1$ and the following overlap integral:

$$\int_{-\infty}^{\infty} f_i^*(t)f_j(t)dt \equiv \langle f_i|f_j\rangle\;. \tag{3.5}$$

These inner products $\langle f_i|f_j\rangle$ define the *indistinguishability* of the photons generated by the related sources. Without loss of generality, the distinguishability is defined to be real, and thus $\langle f_i|f_j\rangle = \langle f_j|f_i\rangle$. When two photons are generated in the same single photon source, $\langle f_i|f_i\rangle = 1$, as the functions are properly normalized. If, however, the photons are completely distinguishable, $\langle f_i|f_j\rangle$ yields 0. Therefore the distinguishability between two photons $0 \leq \langle f_i|f_j\rangle \leq 1$. In addition, it will be really useful to define further variables, α_{ij} and β_{ij}, which represent the distinguishability of photons from the same station and opposite, respectively:

$$\begin{aligned}
&\alpha_{12} \equiv \langle f_1|f_2\rangle\,, \quad \alpha_{34} \equiv \langle f_3|f_4\rangle\,, \\
&\beta_{13} \equiv \langle f_1|f_3\rangle\,, \quad \beta_{14} \equiv \langle f_1|f_4\rangle\,, \quad \beta_{23} \equiv \langle f_2|f_3\rangle\,, \quad \beta_{24} \equiv \langle f_2|f_4\rangle\;.
\end{aligned} \tag{3.6}$$

Let us calculate now the following expectation value

$$\begin{aligned}
\left\langle \hat{a}_{f_i}(t)\hat{a}^\dagger_{f_j}(t')\right\rangle &= \left\langle \int_{-\infty}^{\infty} f_i(t)a(t)dt \cdot \int_{-\infty}^{\infty} f_j^*(t')a^\dagger(t')dt'\right\rangle = \iint_{-\infty}^{\infty} f_i(t)f_j^*(t')\left\langle a(t)a^\dagger(t')\right\rangle dtdt' \\
&= \iint_{-\infty}^{\infty} f_i(t)f_j^*(t')\delta(t-t')dtdt' = \int_{-\infty}^{\infty} f_i(t)f_j^*(t)dt = \langle f_j|f_i\rangle = \langle f_i|f_j\rangle\;.
\end{aligned} \tag{3.7}$$

Even though both operators belong to the same mode defined before, their temporal modes are different. This means that only for completely indistinguishable photons we will obtain $\left\langle \hat{a}_{f_i}(t)\hat{a}^\dagger_{f_j}(t')\right\rangle = 1$ as follows from the relations given in equation 3.7, whereas for distinguishable photons the expected value yields zero. One can guess already the impact that the use of distinguishable photons could have on the results obtained in the previous chapter.

Similarly, we recalculate equation 3.2 with the time dependent operators

$$\left\langle \hat{a}_{f_i}(t)\hat{a}_{f_j}(t')\hat{a}^\dagger_{f_k}(t'')\hat{a}^\dagger_{f_l}(t''')\right\rangle = \iiiint_{-\infty}^{\infty} f_i(t)f_j(t')f_k^*(t'')f_l^*(t''')dtdt'dt''dt'''\left\langle a(t)a(t')a^\dagger(t'')a^\dagger(t''')\right\rangle, \tag{3.8}$$

and by making use of the commutation relations from equation (3.3) we obtain

$$\begin{aligned}
&\left\langle \hat{a}_{f_i}(t)\hat{a}_{f_j}(t')\hat{a}^\dagger_{f_k}(t'')\hat{a}^\dagger_{f_l}(t''')\right\rangle = \left\langle \hat{a}_{f_i}(t)\left(\delta(t'-t'') + \hat{a}^\dagger_{f_k}(t'')\hat{a}_{f_j}(t')\right)\hat{a}^\dagger_{f_l}(t''')\right\rangle \\
&= \iiiint_{-\infty}^{\infty} f_i(t)f_j(t')f_k^*(t'')f_l^*(t''')\delta(t'-t'')\left\langle a(t)a^\dagger(t''')\right\rangle dtdt'dt''dt''' \\
&+ \iiiint_{-\infty}^{\infty} f_i(t)f_j(t')f_k^*(t'')f_l^*(t''')\left\langle a(t)a^\dagger(t'')\right\rangle\left\langle a(t')a^\dagger(t''')\right\rangle dtdt'dt''dt''' \\
&= \iiiint_{-\infty}^{\infty} f_i(t)f_j(t')f_k^*(t'')f_l^*(t''')\delta(t'-t'')\delta(t-t''')dtdt'dt''dt''' \\
&+ \iiiint_{-\infty}^{\infty} f_i(t)f_j(t')f_k^*(t'')f_l^*(t''')\delta(t-t'')\delta(t'-t''')dtdt'dt''dt''' \\
&= \iint_{-\infty}^{\infty} f_i(t)f_j(t')f_k^*(t')f_l^*(t)dtdt' + \iint_{-\infty}^{\infty} f_i(t)f_j(t')f_k^*(t)f_l^*(t')dtdt' \\
&= \langle f_i|f_l\rangle\langle f_j|f_k\rangle + \langle f_i|f_k\rangle\langle f_j|f_l\rangle\ .
\end{aligned} \tag{3.9}$$

Therefore, in the case when photons share the same temporal modes (which is the inner product that will arise more often throughout the thesis), one obtains

$$\left\langle \hat{a}_{f_i}(t)\hat{a}_{f_j}(t')\hat{a}^\dagger_{f_i}(t'')\hat{a}^\dagger_{f_j}(t''')\right\rangle = 1 + |\langle f_i|f_j\rangle|^2\,. \tag{3.10}$$

Note that the above expectation value = 2 only when we consider indistinguishable photons. Otherwise, the matrix element value will stand between 1 and 2.

Let us next calculate an example that mixes both situations: photons with different polarization and different temporal modes. To begin with, we apply the initial commutation relations (equation 3.1), by recalling that the operators corresponding to different polarization modes commute, and the results obtained in equations 3.7 and 3.10 along with 3.6:

$$\left\langle \hat{q}_{H_{f_1}}\hat{q}_{V_{f_3}}\hat{q}_{V_{f_4}}\hat{q}^\dagger_{H_{f_2}}\hat{q}^\dagger_{V_{f_3}}\hat{q}^\dagger_{V_{f_4}}\right\rangle = \left\langle \hat{q}_{H_{f_1}}\hat{q}^\dagger_{H_{f_2}}\right\rangle\left\langle \hat{q}_{V_{f_3}}\hat{q}_{V_{f_4}}\hat{q}^\dagger_{V_{f_3}}\hat{q}^\dagger_{V_{f_4}}\right\rangle = \alpha_{12}(1+\alpha_{34}^2)\,. \tag{3.11}$$

For completeness and given that it will be necessary in the following chapters, one can calculate as well (ommitting the time dependence in the operators to simplify the notation):

$$\begin{aligned}
\left\langle \hat{a}_{f_i}\hat{a}_{f_j}\hat{a}_{f_k}\hat{a}^\dagger_{f_l}\hat{a}^\dagger_{f_m}\hat{a}^\dagger_{f_n}\right\rangle &= \langle f_i|f_l\rangle\left[\langle f_j|f_m\rangle\langle f_k|f_n\rangle + \langle f_j|f_n\rangle\langle f_k|f_m\rangle\right] \\
&+ \langle f_j|f_l\rangle\left[\langle f_i|f_m\rangle\langle f_k|f_n\rangle + \langle f_i|f_n\rangle\langle f_k|f_m\rangle\right] \\
&+ \langle f_k|f_l\rangle\left[\langle f_i|f_m\rangle\langle f_j|f_n\rangle + \langle f_i|f_n\rangle\langle f_j|f_m\rangle\right]\,.
\end{aligned} \tag{3.12}$$

It will be useful, again, to substitute in 3.12 the case when $i = l$, $j = m$ and $k = n$. It reduces to:

$$\left\langle \hat{a}_{f_i}\hat{a}_{f_j}\hat{a}_{f_k}\hat{a}^\dagger_{f_i}\hat{a}^\dagger_{f_j}\hat{a}^\dagger_{f_k}\right\rangle = 1 + |\langle f_i|f_j\rangle|^2 + |\langle f_i|f_k\rangle|^2 + |\langle f_j|f_k\rangle|^2 + 2\langle f_i|f_j\rangle\langle f_j|f_k\rangle\langle f_k|f_i\rangle\ . \tag{3.13}$$

We have thus described how we will model the distinguishability of photons by taking into account the time dependence of the creation operators and defining the convoluting functions $f_i(t)$. We are able to quantify the degree of distinguishability with the parameters α and β, which take the limiting value of 0 for completely distinguishable photons and 1 for the indistinguishable case. However, how can one measure them? So far, they only relate the overlap of these functions abstractly. In the next section, we will find a relation between them and an actual observable: the visibility of the sources.

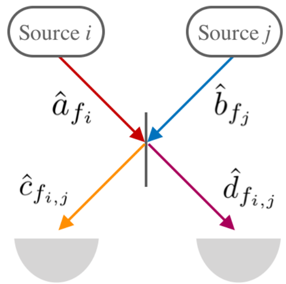

Figure 3.1: Realization of Hong-Ou-Mandel interferometry to calculate the visibility of the sources i and j. The beam splitter has 50:50 probability of transmission/reflection.

3.2 Visibility and distinguishability

The visibility of the sources is measured experimentally by Hong-Ou-Mandel interferometry. One can perform the interference by pairing the sources that form part of the set-up in all possible combinations (with four single-photon sources, there are 8 different visibilities to measure) and thus obtain all the visibilities accurately. We will prove that those visibilities correspond to the parameters α_{ij} and β_{ij} defined in the previous section. Following Figure 3.1, the incoming beams emmitted by the pair of sources are represented by the operators $\hat{a}$ and $\hat{b}$, respectively. Each of them has a different temporal shape, as defined in equation 3.4:

$$\hat{a}_{f_i}(t) = \int_{-\infty}^{\infty} f_i(t)\hat{a}(t)dt, \quad \hat{b}_{f_j}(t) = \int_{-\infty}^{\infty} f_j(t)\hat{b}(t)dt\,. \tag{3.14}$$

They are transformed by the 50:50 beam splitter of the interferometer as

$$\hat{a}^\dagger_{f_i} = \frac{1}{\sqrt{2}}\left(i\hat{c}^\dagger_{f_i} + \hat{d}^\dagger_{f_i}\right), \quad \hat{b}^\dagger_{f_j} = \frac{1}{\sqrt{2}}\left(\hat{c}^\dagger_{f_j} + i\hat{d}^\dagger_{f_j}\right). \tag{3.15}$$

Therefore, the input state $|\psi_{in}\rangle = \hat{a}^\dagger_{f_i}\hat{b}^\dagger_{f_j}|\emptyset\rangle$ to the interferometer leads to the output state after the 50:50 beam splitter:

$$|\psi_{in}\rangle = \hat{a}^\dagger_{f_i}\hat{b}^\dagger_{f_j}|\emptyset\rangle \to |\psi_{out}\rangle = \frac{1}{2}\left(i\hat{c}^\dagger_{f_i}\hat{c}^\dagger_{f_j} - \hat{c}^\dagger_{f_i}\hat{d}^\dagger_{f_j} + \hat{c}^\dagger_{f_j}\hat{d}^\dagger_{f_i} + i\hat{d}^\dagger_{f_i}\hat{d}^\dagger_{f_j}\right)|\emptyset\rangle \tag{3.16}$$

We are interested in the coincidence counts (cc), this is, when both detectors click simultaneously, reducing the output state to $|\psi^{cc}_{out}\rangle = \frac{1}{2}\left(\hat{c}^\dagger_{f_j}\hat{d}^\dagger_{f_i} - \hat{c}^\dagger_{f_i}\hat{d}^\dagger_{f_j}\right)|\emptyset\rangle$. The probability for coincidence counts to occur then evaluates to

$$\begin{aligned}
P_{cc} = \langle\psi^{cc}_{out}|\psi^{cc}_{out}\rangle &= \frac{1}{4}\left\langle\left(\hat{c}_{f_j}\hat{d}_{f_i} - \hat{c}_{f_i}\hat{d}_{f_j}\right)\left(\hat{c}^\dagger_{f_j}\hat{d}^\dagger_{f_i} - \hat{c}^\dagger_{f_i}\hat{d}^\dagger_{f_j}\right)\right\rangle \\
&= \frac{1}{4}\left(\left\langle\hat{c}_{f_j}\hat{c}^\dagger_{f_j}\right\rangle\left\langle\hat{d}_{f_i}\hat{d}^\dagger_{f_i}\right\rangle - \left\langle\hat{c}_{f_j}\hat{c}^\dagger_{f_i}\right\rangle\left\langle\hat{d}_{f_i}\hat{d}^\dagger_{f_j}\right\rangle - \left\langle\hat{c}_{f_i}\hat{c}^\dagger_{f_j}\right\rangle\left\langle\hat{d}_{f_j}\hat{d}^\dagger_{f_i}\right\rangle + \left\langle\hat{c}_{f_i}\hat{c}^\dagger_{f_i}\right\rangle\left\langle\hat{d}_{f_j}\hat{d}^\dagger_{f_j}\right\rangle\right) \\
&= \frac{1}{2}\left(1 - |\langle f_i|f_j\rangle|^2\right).
\end{aligned} \tag{3.17}$$

This means that the probability for both detectors to click at the same time depends on the degree of indistinguishability of the incoming photons. This agrees with the cases introduced previously for HOM: when photons are indistinguishable, $\langle f_i|f_j\rangle = 1$ and thus the probability of coincidence counts is zero. As they bunch together in the beam splitter, they will both click either at one or the other detector. On the other hand, if we identify the modes i and j with orthogonal polarizations, then photons are completely distinguishable ($\langle f_i|f_j\rangle = 0$) and therefore there is equal probability for coincidence counts and clicks on different detectors, as discussed in the Introduction. The probability $P_{max} = P_{cc}(\langle f_i|f_j\rangle = 0) = 1/2$ is the maximum value that it can reach. Given the distinguishability of photons, the minimum one is precisely P_{cc}. We can then calculate the visibility V of the sources [35]:

$$V = \frac{P_{max} - P_{min}}{P_{max}} = \frac{\frac{1}{2} - \frac{1}{2}\left(1 - |\langle f_i|f_j\rangle|^2\right)}{\frac{1}{2}} = |\langle f_i|f_j\rangle|^2 . \tag{3.18}$$

Equation 3.18 relates the distinguishability of the photons with the visibility of the sources that generated them. This way we can fully describe with actual measurable quantities the temporal evolution of our operators and the density matrix of the system.

3.3 Losses

The loss of photons always plays an important role in any optical experiment. In this section we will model this possibility, as well as calculate its impact on the success of the protocol. When the final state was calculated in the previous chapter, we already introduced one type of loss: a transmission loss between Alice and Bob and the heralding station (equation 2.9). However, the option for the photon to get lost on its way to the heralding station does not affect the success of the protocol itself. It rather only influences the key rate, that is, a low transmission rate will imply that many photons will have to be sent before we can generate a succesful entangled pair. Is this also the case if the photon gets lost even *before* it is transmitted to the CHS or, alternatively, while being measured? In Chapter 1, we considered only the desired case for the CHS station where one photon from Alice and another from Bob arrived at the same time with orthogonal polarizations at

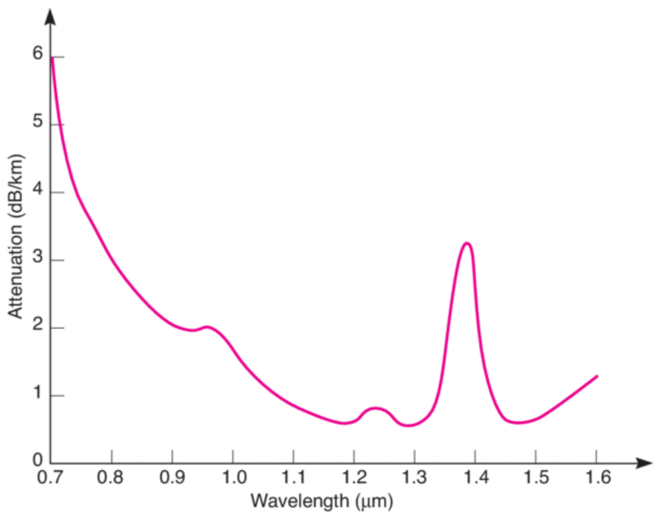

Figure 3.2: Typical spectral attenuation in Silica. Source: [5]

different PBS. If two photons arrived to the heralding station and gave an incorrect combination of clicks, the event was disregarded; if the combination was correct, we were guaranteed the success of the event. Note that, even if Alice or Bob does not receive any photons to measure, they need to consider a strategy to account for this photon loss process that will indeed affect the success of the protocol. New creation operators describing the photons lost from the set-up at different points are therefore needed.

3.3.1 Transmission losses

The loss of photons during the transmission from Alice and Bob's stations to the heralding station is due to the attenuation of the optical fiber. The attenuation, in general defined by a coefficient α, is given in dB and is due to absorption, scattering, bending of the fiber and interface inhomogeneities of the medium in which photons are transmitted. This is the reason why the attenuation coefficient is naturally dependent on the wavelength of the transmitted photons (see Figure 3.2). It is defined as

$$\alpha = -\frac{10}{z(km)} \log \frac{P(z)}{P(0)} \,, \tag{3.19}$$

where z is the distance, typically given in kms, that the photons travel with the rate of optical power at the point where photons where emitted ($P(0)$) and received ($P(z)$) [44]. The transmission efficiency η_t that was already used in the previous chapter is precisely this rate, given that it represents the probability for the photons to travel succesfully the distance z. In fact, from equation 3.19:

$$\eta_t \equiv \frac{P(z)}{P(0)} = 10^{-\alpha \frac{z(km)}{10}} \,. \tag{3.20}$$

The probability of transmission is, thus, very low for long distances. For example, let us consider the natural emission wavelength of a InGaAs quantum dot, 0.95μm [45], which according to Figure 3.2 leads to an attenuation factor of 2 dB. If there is a distance of 10 km between Alice and Bob and the heralding station, applying equation 3.20 a value of $\eta_t \approx 0.1$ is obtained. This means, only one in 100 photons will arrive succesfully to the heralding station. Under these conditions, it becomes irrelevant to account for different transmission efficiencies for each emmitted photons and one transmission coefficient interpreted as approximately identical for all of them can be used.

3.3.2 Local losses

It was pointed out above that it is necessary to introduce further efficiency parameters. With this purpose, $\eta_{1_{fi}}$ is defined as the probability of the photons to arrive succesfully from the source that generated them to the first beam splitter and $\eta_{2_{fi}}$ is the probability for the reflected ones to be detected as sketched in Figure 3.3. The local efficiency $\eta_{l_{fi}}$ is thus defined as

$$\eta_{l_{fi}} \equiv \eta_{1_{fi}} \eta_{2_{fi}} (1 - T) \,. \tag{3.21}$$

Note that the different probabilities of transmission within Alice and Bob's stations do depend in this case on the source of the specific photon. This accounts for possible assymetries in the local transmission at Alice and Bob's laboratories, as well as different responses of the optical devices to the photons depending on where they were generated. Furthermore, we can try to estimate a typical value of the local efficiency. Regarding the probability of photons to reach the first beam splitter, it will mainly depend on the coupling efficiency from the quantum dot to the corresponding nanophotonic waveguide (we will neglect the absorption of the optical fiber within the local stations, as the distances are not comparable to the distance between them and the heralding station). This coupling efficiency has been proven to reach up to 98% [38]. However, the coupling efficiency from the waveguide to the optical fiber has tipically a 60% efficiency [4]. On the other hand, η_2 will be limited by the reflectance of the wave-plates. The reflectance of wave-plates can vary between 0.25% and 0.5% depending on whether they are made of quartz or a liquid crystal polymer (LCP) [46]. With all these numbers and a low transmittance of the beam splitter ($T \approx 0.1$) we can compute an estimation of the local efficiency, giving $\eta_{l_{fi}} \approx 58\%$.

3.3.3 Theoretical model

The transformation of the initial creation operators needs to include new creation operators that describe all the possible processes corresponding to the loss of photons. They are defined as $\hat{a}^\dagger_{\gamma_{j_{fi}}}$, and indexed depending on the source that generated them (f_i) and where the photon got lost ($j = 1, 2, t$). The transformation associated with the loss of a photon has the following normalized structure:

$$\hat{a}^\dagger_{fi} \to \sqrt{\eta_{j_{fi}}}\hat{a}^\dagger_{fi} + \sqrt{1-\eta_{j_{fi}}}\hat{a}^\dagger_{\gamma_{j_{fi}}} . \tag{3.22}$$

We next define an operator $\hat{L}^\dagger_{fi}$, that represents all the possible lost photons that were generated in the same source:

$$\hat{L}^\dagger_{fi} \equiv \sqrt{1-\eta_{1_{fi}}}\hat{a}^\dagger_{\gamma_{1_{fi}}} + i\sqrt{\eta_{1_{fi}}(1-\eta_{2_{f1}})(1-T)}\hat{a}^\dagger_{\gamma_{2_{fi}}} + \sqrt{\eta_{1_{fi}}(1-\eta_t)T}\hat{a}^\dagger_{\gamma_{t_{fi}}} . \tag{3.23}$$

It will be relevant for the upcoming calculations to calculate the following expected values (note that all the photon operators from different zones of emission commute, as well as the ones with different polarization or proceeding from different labs):

$$\begin{aligned}\left\langle \hat{L}_{fi}\hat{L}^\dagger_{fi}\right\rangle &= 1-\eta_{1_{fi}} + \eta_{1_{fi}}(1-\eta_{2_{fi}})(1-T) + \eta_{1_{fi}}(1-\eta_t)T = \\ &= 1-\eta_{1_{fi}}\eta_{2_{fi}}(1-T) - \eta_{1_{fi}}\eta_t T ,\end{aligned} \tag{3.24}$$

which is the probability for one photon to get lost. One can read equation 3.24 as 1 minus all the probabilities of photons arriving succesfully to detection, $\eta_{1_{fi}}\eta_{2_{fi}}(1-T)$, or to the heralding station, $\eta_{1_{fi}}\eta_t T$. Note that $\left\langle \hat{L}_{fi}\hat{L}^\dagger_{fj}\right\rangle_{i\neq j} = 0$. This is due to the fact that the creation operators

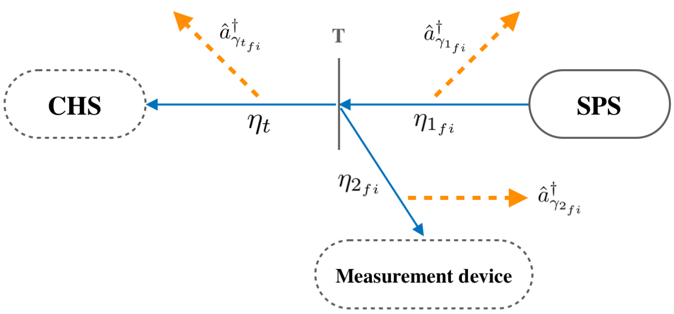

Figure 3.3: Simple sketch that shows to which part of the set-up is every efficiency η assigned, as well as the lost photons (represented by their creation operators). Every value of η also depends on the source which emitted the photon.

of lost photons generated at different sources always lead to an expectation value equal to 0, as they either come from different labs (expectation values of the form $\left\langle \hat{a}_{fi}\hat{b}^{\dagger}_{fj}\right\rangle = 0$) or, if they were generated in the same station, they would have orthogonal polarization, leading to 0 as well. Similarly, we can calculate the expectation value for two lost photons

$$\begin{aligned}\left\langle \hat{L}_{fi}\hat{L}_{fj}\hat{L}^{\dagger}_{fi}\hat{L}^{\dagger}_{fj}\right\rangle = &(1-\eta_{1_{fi}})(1-\eta_{1_{fj}}) + (1-\eta_{1_{fi}})\eta_{1_{fj}}(1-\eta_{2_{fj}})(1-T) + (1-\eta_{1_{fi}})\eta_{1_{fj}}(1-\eta_t)T\\ &+\eta_{1_{fi}}(1-\eta_{1_{fj}})(1-\eta_{2_{fi}})(1-T) + \eta_{1_{fi}}\eta_{1_{fj}}(1-\eta_{2_{fi}})(1-\eta_{2_{fj}})(1-T)^2+\\ &+\eta_{1_{fi}}\eta_{1_{fj}}(1-\eta_{2_{fi}})(1-\eta_t)T(1-T) + \eta_{1_{fi}}(1-\eta_{1_{fj}})(1-\eta_t)T\\ &+\eta_{1_{fi}}\eta_{1_{fj}}(1-\eta_{2_{fj}})(1-\eta_t)T(1-T) + \eta_{1_{fi}}\eta_{1_{fj}}(1-\eta_t)^2T^2\,,\end{aligned} \tag{3.25}$$

which simplifies to

$$\begin{aligned}\left\langle \hat{L}_{fi}\hat{L}_{fj}\hat{L}^{\dagger}_{fi}\hat{L}^{\dagger}_{fj}\right\rangle &= (1-\eta_{1_{fi}}\eta_{2_{fi}}(1-T)-\eta_{1_{fi}}\eta_t T)(1-\eta_{1_{fj}}\eta_{2_{fj}}(1-T)-\eta_{1_{fj}}\eta_t T)\\ &= \left\langle \hat{L}_{fi}\hat{L}^{\dagger}_{fi}\right\rangle\left\langle \hat{L}_{fj}\hat{L}^{\dagger}_{fj}\right\rangle\,.\end{aligned} \tag{3.26}$$

As expected, $\left\langle \hat{L}_{fi}\hat{L}_{fj}\hat{L}^{\dagger}_{fi}\hat{L}^{\dagger}_{fj}\right\rangle$ is simply the product of the probabilities of the lost photons i and j. Indeed, we could have arrived to this result directly, as the creation operators of photons generated in different sources commute. Furthermore, note that $\left\langle \hat{L}_{fi}\hat{L}_{fj}\hat{L}^{\dagger}_{fk}\hat{L}^{\dagger}_{fl}\right\rangle_{i\neq k, j\neq l} = 0$ holds indeed from equation 3.24. Now the whole transformation for the initial creation operators is completed by adding the two extra mechanisms of loss with equation 3.22 and is found to be:

$$\begin{aligned}\hat{a}^{\dagger}_{H_{f1}} &\rightarrow \sqrt{\frac{\eta_{1_{f1}}\eta_t T}{2}}\hat{O}^{\dagger}_{f1} + i\sqrt{\eta_{1_{f1}}\eta_{2_{f1}}(1-T)}\hat{a}^{\dagger}_{H_{f1}} + \hat{L}^{\dagger}_{f1},\\ \hat{a}^{\dagger}_{V_{f2}} &\rightarrow \sqrt{\frac{\eta_{1_{f2}}\eta_t T}{2}}\hat{O}^{\dagger}_{f2} + i\sqrt{\eta_{1_{f2}}\eta_{2_{f2}}(1-T)}\hat{a}^{\dagger}_{V_{f2}} + \hat{L}^{\dagger}_{f2},\\ \hat{b}^{\dagger}_{H_{f3}} &\rightarrow \sqrt{\frac{\eta_{1_{f3}}\eta_t T}{2}}\hat{O}^{\dagger}_{f3} + i\sqrt{\eta_{1_{f3}}\eta_{2_{f3}}(1-T)}\hat{b}^{\dagger}_{H_{f3}} + \hat{L}^{\dagger}_{f3},\\ \hat{b}^{\dagger}_{V_{f4}} &\rightarrow \sqrt{\frac{\eta_{1_{f4}}\eta_t T}{2}}\hat{O}^{\dagger}_{f4} + i\sqrt{\eta_{1_{f4}}\eta_{2_{f4}}(1-T)}\hat{b}^{\dagger}_{V_{f4}} + \hat{L}^{\dagger}_{f4}\,,\end{aligned} \tag{3.27}$$

where the following operators have been defined representing the creation of the photons that arrive to the heralding station:

$$\begin{aligned}\hat{O}^{\dagger}_{f1} &\equiv i\sqrt{1-t}(p^{\dagger}_{H_{f1}} + p^{\dagger}_{V_{f1}}) + \sqrt{t}(q^{\dagger}_{H_{f1}} + q^{\dagger}_{V_{f1}}),\\ \hat{O}^{\dagger}_{f2} &\equiv i\sqrt{1-t}(p^{\dagger}_{H_{f2}} - p^{\dagger}_{V_{f2}}) + \sqrt{t}(q^{\dagger}_{H_{f2}} - q^{\dagger}_{V_{f2}}),\\ \hat{O}^{\dagger}_{f3} &\equiv \sqrt{t}(p^{\dagger}_{H_{f3}} + p^{\dagger}_{V_{f3}}) + i\sqrt{1-t}(q^{\dagger}_{H_{f3}} + q^{\dagger}_{V_{f3}}),\\ \hat{O}^{\dagger}_{f4} &\equiv \sqrt{t}(p^{\dagger}_{H_{f4}} - p^{\dagger}_{V_{f4}}) + i\sqrt{1-t}(q^{\dagger}_{H_{f4}} - q^{\dagger}_{V_{f4}})\,.\end{aligned} \tag{3.28}$$

We have thus written the whole transformation of the initial creation operators in a very compact and clear way: each photon has a certain probability to click in the heralding station ($\hat{O}^{\dagger}_{fi}$), to be detected at the local measurement station ($\hat{a}^{\dagger}_{fi}$ and $\hat{b}^{\dagger}_{fi}$) or to get lost ($\hat{L}^{\dagger}_{fi}$). This representation of the transformation will allow us in Chapters 4 and 5 to separate clearly all the different events that influence the protocol introduced in Chapter 2. As we did with the $\hat{L}^{\dagger}_{fi}$ operators, it will be very useful to calculate the expectation values of the creation operators at the heralding station. These calculations are detailed in section 5.2.1.

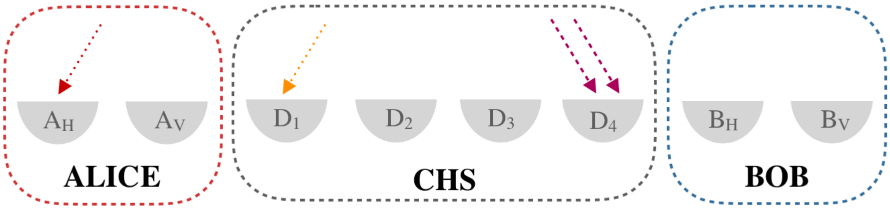

Figure 3.4: Example of a multiphoton detection event. The heralding station receives what it considers a succesful event. However, two photons clicked on D_4 instead of one, providing Alice and Bob with misleading information about the quality of their shared pair of photons as in reality Bob will not detect any.

3.4 Multiphoton detection

Unfortunately, detectors that can resolve the number of detected photons are expensive and not very common in most of photonic experiments. Instead, most photodetectors give a response when light arrives, indistinctively of how many photons did. This gives rise to a simple problem: so far we have based the success of the protocol on the fact that once the heralding station receives the valid combination of clicks, Alice and Bob can ensure that they share an entangled pair. However, if the heralding station can not differentiate between whether one or two photons clicked on the same detector with the correct combination, it will be taken as a successful event by Alice and Bob although the combination is, essentially, incorrect. Let us consider an example. There is a fair probability that the two photons generated in the same station are transmitted to the CHS. If we imagine a scenario in which both photons generated by Bob are trasmitted to the heralding station and only one from Alice's station, a situation like the one depicted in Figure 3.4 can occur. One photon clicked on detector D_1 and two clicked simultaneously on detector D_4. The detector can not distinguish the number of photons that clicked on D_4, implying that the heralding station reckons the valid combination D_1D_4. Consequently, it will transmit to Alice and Bob that the state they share is correct, but Bob will detect no photon. This will be an important source of noise in the protocol and all the different contributions will be discussed carefully in Chapter 5.

Chapter 4

Effect of the distinguishability of photons

So far, we have assumed that the photons emitted by the sources are indistinguishable beyond their polarization, as it has been considered in [2]. This does not have to be necessarily true. Each of the sources can add noise on top of the single photon wavepacket, making it clearly distinguishable from the others and therefore affecting their final interference. The objective of this chapter is to calculate quantitatively the effect of how much the emmitted photons can be distinguished and how it can potentially influence the success of the protocol. The rest of errors introduced in the previous chapter (losses and multiphoton detection) are not included yet.

4.1 Transformation of the time-dependent creation operators

We in this section consider photons coming from the sources at Alice and Bob's stations with different polarizations and temporal modes. They are no longer indistinguishable and due to this, the state shared by the entangled pair in possesion of Alice and Bob can no longer be represented by equation 2.23. Instead, the quality of the state will depend on the HOM visibility, written in terms of the inner products $\langle f_i|f_j\rangle$. Each source has one function $f_i(t)$ associated (see table 4.1), with the creation operator for the photons coming from that source. The transformation of the creation operators is exactly the same as in Chapter 1 with each of the operators now carrying

	Polarization	Function	Creation operator
Alice	H	$f_1(t)$	$\hat{a}^\dagger_{sH_{f1}}$
	V	$f_2(t)$	$\hat{a}^\dagger_{sV_{f2}}$
Bob	H	$f_3(t)$	$\hat{b}^\dagger_{sH_{f3}}$
	V	$f_4(t)$	$\hat{b}^\dagger_{sV_{f4}}$

Table 4.1: Brief explanation about the notation of the creation operators of the photons and its procedence: polarization and original source, providing with four different temporal modes $f_i(t)$.

the label indicating its temporal mode as shown in table 4.1. The photon operators at Alice and Bob's stations corresponding to the transformation at the central heralding station then becomes

$$
\begin{aligned}
\hat{a}^{\dagger}_{sH_{f1}} &\to \sqrt{\frac{\eta_t T}{2}}(i\sqrt{1-t}(\hat{p}^{\dagger}_{H_{f1}}+\hat{p}^{\dagger}_{V_{f1}})+\sqrt{t}(\hat{q}^{\dagger}_{H_{f1}}+\hat{q}^{\dagger}_{V_{f1}}))+i\sqrt{1-T}\hat{a}^{\dagger}_{H_{f1}},\\
\hat{a}^{\dagger}_{sV_{f2}} &\to \sqrt{\frac{\eta_t T}{2}}(i\sqrt{1-t}(\hat{p}^{\dagger}_{H_{f2}}-\hat{p}^{\dagger}_{V_{f2}})+\sqrt{t}(\hat{q}^{\dagger}_{H_{f2}}-\hat{q}^{\dagger}_{V_{f2}}))+i\sqrt{1-T}\hat{a}^{\dagger}_{V_{f2}},\\
\hat{b}^{\dagger}_{sH_{f3}} &\to \sqrt{\frac{\eta_t T}{2}}(\sqrt{t}(\hat{p}^{\dagger}_{H_{f3}}+\hat{p}^{\dagger}_{V_{f3}})+i\sqrt{1-t}(\hat{q}^{\dagger}_{H_{f3}}+\hat{q}^{\dagger}_{V_{f3}}))+i\sqrt{1-T}\hat{b}^{\dagger}_{H_{f3}},\\
\hat{b}^{\dagger}_{sV_{f4}} &\to \sqrt{\frac{\eta_t T}{2}}(\sqrt{t}(\hat{p}^{\dagger}_{H_{f4}}-\hat{p}^{\dagger}_{V_{f4}})+i\sqrt{1-t}(\hat{q}^{\dagger}_{H_{f4}}-\hat{q}^{\dagger}_{V_{f4}}))+i\sqrt{1-T}\hat{b}^{\dagger}_{V_{f4}}\,.
\end{aligned}
\tag{4.1}
$$

The main difference now that the distinguishability of photons has been introduced is that there will be many crossed terms that will not cancel anymore. For example, $-\hat{p}^{\dagger}_{H_{f1}}\hat{p}^{\dagger}_{V_{f2}}+\hat{p}^{\dagger}_{H_{f2}}\hat{p}^{\dagger}_{V_{f1}}$ would cancel in the indistinguishable limit but they do not with different temporal modes. Recall that it is the same situation that was explored when HOM was introduced: paths do not interfere destructively anymore once one can distinguish one photon from the other. Like in Chapter 1, we keep again those terms that are multiplied by the coefficient $\sqrt{\frac{\eta_t T(1-T)}{2}}$, because those are the only ones that can lead to succesful events (one photon staying in the station where it was generated and another arriving to the CHS):

$$
\begin{aligned}
\hat{a}^{\dagger}_{sH_{f1}}\hat{a}^{\dagger}_{sV_{f2}} &\to i\sqrt{\frac{\eta_t T(1-T)}{2}}(i\sqrt{1-t}((\hat{p}^{\dagger}_{H_{f1}}+\hat{p}^{\dagger}_{V_{f1}})\hat{a}^{\dagger}_{V_{f2}}+(\hat{p}^{\dagger}_{H_{f2}}-\hat{p}^{\dagger}_{V_{f2}})\hat{a}^{\dagger}_{H_{f1}})\\
&+\sqrt{t}((\hat{q}^{\dagger}_{H_{f1}}+\hat{q}^{\dagger}_{V_{f1}})\hat{a}^{\dagger}_{V_{f2}}+(\hat{q}^{\dagger}_{H_{f2}}-\hat{q}^{\dagger}_{V_{f2}})\hat{a}^{\dagger}_{H_{f1}})),\\
\hat{b}^{\dagger}_{sH_{f3}}\hat{b}^{\dagger}_{sV_{f4}} &\to i\sqrt{\frac{\eta_t T(1-T)}{2}}(i\sqrt{1-t}((\hat{q}^{\dagger}_{H_{f3}}+\hat{q}^{\dagger}_{V_{f3}})\hat{b}^{\dagger}_{V_{f4}}+(\hat{q}^{\dagger}_{H_{f4}}-\hat{q}^{\dagger}_{V_{f4}})\hat{b}^{\dagger}_{H_{f3}})\\
&+\sqrt{t}((\hat{p}^{\dagger}_{H_{f3}}+\hat{p}^{\dagger}_{V_{f3}})\hat{b}^{\dagger}_{V_{f4}}+(\hat{p}^{\dagger}_{H_{f4}}-\hat{p}^{\dagger}_{V_{f4}})\hat{b}^{\dagger}_{H_{f3}}))\,.
\end{aligned}
\tag{4.2}
$$

As in the indistinguishable limit, we focus on two-click combinations, specifically those corresponding to photons that arrive simultaneously to different PBS and with orthogonal polarizations. Furthermore, in order to clarify the notation, the following operators are defined[1] as

$$
\begin{aligned}
\hat{\Theta}^{\dagger}_1 &\equiv (1-t)\left(\hat{p}^{\dagger}_{H_{f2}}\hat{q}^{\dagger}_{V_{f4}}+\hat{p}^{\dagger}_{V_{f2}}\hat{q}^{\dagger}_{H_{f4}}\right)+t\left(-\hat{p}^{\dagger}_{V_{f4}}\hat{q}^{\dagger}_{H_{f2}}-\hat{p}^{\dagger}_{H_{f4}}\hat{q}^{\dagger}_{V_{f2}}\right),\\
\hat{\Theta}^{\dagger}_2 &\equiv (1-t)\left(-\hat{p}^{\dagger}_{H_{f2}}\hat{q}^{\dagger}_{V_{f3}}+\hat{p}^{\dagger}_{V_{f2}}\hat{q}^{\dagger}_{H_{f3}}\right)+t\left(\hat{p}^{\dagger}_{V_{f3}}\hat{q}^{\dagger}_{H_{f2}}-\hat{p}^{\dagger}_{H_{f3}}\hat{q}^{\dagger}_{V_{f2}}\right),\\
\hat{\Theta}^{\dagger}_3 &\equiv (1-t)\left(\hat{p}^{\dagger}_{H_{f1}}\hat{q}^{\dagger}_{V_{f4}}-\hat{p}^{\dagger}_{V_{f1}}\hat{q}^{\dagger}_{H_{f4}}\right)+t\left(-\hat{p}^{\dagger}_{V_{f4}}\hat{q}^{\dagger}_{H_{f1}}+\hat{p}^{\dagger}_{H_{f4}}\hat{q}^{\dagger}_{V_{f1}}\right),\\
\hat{\Theta}^{\dagger}_4 &\equiv (1-t)\left(-\hat{p}^{\dagger}_{H_{f1}}\hat{q}^{\dagger}_{V_{f3}}-\hat{p}^{\dagger}_{V_{f1}}\hat{q}^{\dagger}_{H_{f3}}\right)+t\left(\hat{p}^{\dagger}_{V_{f3}}\hat{q}^{\dagger}_{H_{f1}}+\hat{p}^{\dagger}_{H_{f3}}\hat{q}^{\dagger}_{V_{f1}}\right)\,.
\end{aligned}
\tag{4.3}
$$

The operators $\hat{\Theta}_i$ thus include all the creation of photons at the CHS station, corresponding to

[1] We have already defined operators that account for the distinguishability of photons in the previous chapter. However, they also include more mechanisms of error. We thus considered that, in order to introduce with more clarity how the transformations and measurements are calculated, it is better to write explicitly all the detection operators involved in this chapter and regroup them in the operators $\hat{\Theta}_i$. The operators $\hat{O}_{fi}$, introduced in Chapter 2, are used in the following chapter.

the postselected succesful events, simplifying the global transformation to

$$\hat{a}^{\dagger}_{sH_{f1}}\hat{a}^{\dagger}_{sV_{f2}}\hat{b}^{\dagger}_{sH_{f3}}\hat{b}^{\dagger}_{sV_{f4}} \to -\frac{\eta_t T(1-T)}{2}\left[\hat{a}^{\dagger}_{H_{f1}}\hat{b}^{\dagger}_{H_{f3}}\hat{\Theta}^{\dagger}_1 + \hat{a}^{\dagger}_{H_{f1}}\hat{b}^{\dagger}_{V_{f4}}\hat{\Theta}^{\dagger}_2 + \hat{a}^{\dagger}_{V_{f2}}\hat{b}^{\dagger}_{H_{f3}}\hat{\Theta}^{\dagger}_3 + \hat{a}^{\dagger}_{V_{f2}}\hat{b}^{\dagger}_{V_{f4}}\hat{\Theta}^{\dagger}_4\right], \tag{4.4}$$

where as before $\hat{a}^{\dagger}_{H_{f1}}, \hat{a}^{\dagger}_{V_{f2}}, \hat{b}^{\dagger}_{H_{f3}}, \hat{b}^{\dagger}_{V_{f4}}$ represent the creation operators for the photons arriving to the measuring devices at Alice and Bob's stations. The output state is not going to be as straightforward as last time (a superposition of Bell states) due to all the extra terms that the four distinguishable photons contribute to it.

As in Chapter 1, the density matrix representing the state of the pair shared by Alice and Bob *before* the detectors at the CHS click. With the new notation, it is equivalent to tracing out the operators $\hat{\Theta}_i$. Applying the cyclic property of the trace then we get:

$$\begin{aligned}\rho &= \mathrm{Tr}_{O_i}\left\{\hat{a}^{\dagger}_{H_{f1}}\hat{a}^{\dagger}_{V_{f2}}\hat{b}^{\dagger}_{H_{f3}}\hat{b}^{\dagger}_{V_{f4}}\left|\emptyset\right\rangle\left\langle\emptyset\right|\hat{a}_{H_{f1}}\hat{a}_{V_{f2}}\hat{b}_{H_{f3}}\hat{b}_{V_{f4}}\right\} \\ &= \left\langle\hat{\Theta}_1\hat{\Theta}^{\dagger}_1\right\rangle\hat{a}^{\dagger}_{H_{f1}}\hat{b}^{\dagger}_{H_{f3}}\left|\emptyset\right\rangle\left\langle\emptyset\right|\hat{a}_{H_{f1}}\hat{b}_{H_{f3}} + \left\langle\hat{\Theta}_2\hat{\Theta}^{\dagger}_1\right\rangle\hat{a}^{\dagger}_{H_{f1}}\hat{b}^{\dagger}_{H_{f3}}\left|\emptyset\right\rangle\left\langle\emptyset\right|\hat{a}_{H_{f1}}\hat{b}_{V_{f4}} + \ldots\end{aligned} \tag{4.5}$$

which is a 4 x 4 matrix. Recall that the density matrix is written in the basis[2]:

$$\left\{\hat{a}^{\dagger}_{H_{f1}}\hat{b}^{\dagger}_{H_{f3}}\left|\emptyset\right\rangle, \hat{a}^{\dagger}_{H_{f1}}\hat{b}^{\dagger}_{V_{f4}}\left|\emptyset\right\rangle, \hat{a}^{\dagger}_{V_{f2}}\hat{b}^{\dagger}_{H_{f3}}\left|\emptyset\right\rangle, \hat{a}^{\dagger}_{V_{f2}}\hat{b}^{\dagger}_{V_{f4}}\left|\emptyset\right\rangle\right\}, \tag{4.6}$$

which is both polarization and time dependent. We next calculate the state of the two photons that is created at Alice and Bob's laboratories right before their respective measurement devices. For this purpose we trace out the detectors, i.e. the $\hat{\Theta}_i$ Hilbert space, by calculating all the $\left\langle\hat{\Theta}_i\hat{\Theta}^{\dagger}_j\right\rangle$, with $i, j = 1, 2, 3, 4$. Applying equation (3.10) and (4.3) we get:

$$\begin{aligned}
&\left\langle\hat{\Theta}_1\hat{\Theta}^{\dagger}_1\right\rangle = 2\left(1 - 2t\left(1-t\right)\left(1+\beta^2_{24}\right)\right), \quad \left\langle\hat{\Theta}_2\hat{\Theta}^{\dagger}_2\right\rangle = 2\left(1 - 2t\left(1-t\right)\left(1-\beta^2_{23}\right)\right), \\
&\left\langle\hat{\Theta}^{\dagger}_3\hat{\Theta}^{\dagger}_3\right\rangle = 2\left(1 - 2t\left(1-t\right)\left(1-\beta^2_{14}\right)\right), \quad \left\langle\hat{\Theta}_4\hat{\Theta}^{\dagger}_4\right\rangle = 2\left(1 - 2t\left(1-t\right)\left(1+\beta^2_{13}\right)\right), \\
\\
&\left\langle\hat{\Theta}_1\hat{\Theta}^{\dagger}_4\right\rangle = 2\left(-\alpha_{12}\alpha_{34} + 2t\left(1-t\right)\left(\alpha_{12}\alpha_{34} + \beta_{14}\beta_{23}\right)\right), \\
&\left\langle\hat{\Theta}_2\hat{\Theta}^{\dagger}_3\right\rangle = 2\left(-\alpha_{12}\alpha_{34} + 2t\left(1-t\right)\left(\alpha_{12}\alpha_{34} - \beta_{13}\beta_{24}\right)\right), \\
\\
&\left\langle\hat{\Theta}_1\hat{\Theta}^{\dagger}_2\right\rangle = \left\langle\hat{\Theta}_1\hat{\Theta}^{\dagger}_3\right\rangle = \left\langle\hat{\Theta}_2\hat{\Theta}^{\dagger}_4\right\rangle = \left\langle\hat{\Theta}_3\hat{\Theta}^{\dagger}_4\right\rangle = 0\,.
\end{aligned} \tag{4.7}$$

If we now consider the hermiticity of the density matrix we get all the 16 matrix elements.

In order to visualize better how the ideal state obtained in Chapter 1 has been modified by introducing the distinguishability of photons, we simplify the matrix elements obtained in equation 4.7 choosing a 50:50 beam splitter ($t = 1/2$) in the CHS station. Furthermore, we consider a plausible symmetric limit, in which all the sources belonging to the same station have the same visibility, and the crossed visibilities between Alice and Bob's sources are identical. That is,

[2]This means that the density matrix is written in a basis dependent on both time and polarization. In the following section it will be detailed how the time will be partially traced out. For now, this density matrix is suficient to explore most of the physics that are relevant to the discussion in the present section.

$\alpha_{12} = \alpha_{34} \equiv \alpha$ and $\beta_{13} = \beta_{14} = \beta_{23} = \beta_{24} \equiv \beta$. In this limit, the density matrix yields, after substituting the results from equation 4.7 in equation 4.5:

$$\rho = \frac{{\eta_t}^2 T^2 (1-T)^2}{4} \begin{pmatrix} 1-\beta^2 & 0 & 0 & \beta^2-\alpha^2 \\ 0 & 1+\beta^2 & -(\alpha^2+\beta^2) & 0 \\ 0 & -(\alpha^2+\beta^2) & 1+\beta^2 & 0 \\ \beta^2-\alpha^2 & 0 & 0 & 1-\beta^2 \end{pmatrix} . \tag{4.8}$$

We find from the above density matrix that, if the photons are indistinguishable ($\alpha = \beta = 1$), equation 4.8 gives $\rho = \frac{\eta_t^2 T^2 (1-T)^2}{2} |\psi^-\rangle$. As photons become more and more distinguishable ($\alpha, \beta < 1$) the state is not a pure Bell state anymore and extra terms arise in the density matrix. If one can completely distinguish all photons ($\alpha = \beta = 0$), equation 4.8 equals a perfect statistical mixture: photons do not bunch together at any point in the set up, and thus, entanglement is never generated. The probability of detection is calculated as

$$P_{14,23} = \mathrm{Tr}\{\rho\} = {\eta_t}^2 T^2 (1-T)^2 . \tag{4.9}$$

It can be seen from Eq. 3.9 that the probability does not depend on the distinguishability of photons, as long as the four crossed combinations of visibilities are equal. This makes sense given that it is known beforehand that a pair of horizontal and vertical photons flying from Alice and Bob's stations are required to arrive to the beam splitter at the CHS (even though we do not know who produced which).

In the ideal case studied in the previous chapter, this "distinguishability" in polarization did not affect the probability of the final state. It was expected that the visibility of the sources did not affect either in this case. However, this argument does not hold when the photons are not equally distinguishable and thus the probability of clicks of detectors D_1D_4 and D_2D_3 depends on $\beta_{13}, \beta_{14}, \beta_{23}, \beta_{24}$. In this case the odd distinguishability between the arriving photons generates bunching at the central beam splitter that de-compensates the state and therefore affects the probability of detection. Nevertheless, it can be verified (it will be done in more detail in the following chapters, including losses) that the probability of detection at the CHS including all the possible events is independent of the visibility of the sources and, as calculated before, gives $4{\eta_t}^2 T^2 (1-T)^2$. This can be justified by the fact that the probability for the CHS to detect two clicks should not depend in any case on how distinguishable the photons are, but rather on the probabilities of transmission.

4.2 Measuring the state

Up to this point, the entangled state that has been described is shared by Alice and Bob and corresponds to the pair of photons that stayed in their stations. The information from the CHS about whether the pair has become properly entangled arrives way after the photons are reflected and thus a postselection process of data is needed. In any case, the state shared by both photons has not been measured yet neither by Alice, nor by Bob. In this chapter we address this and recreate a experiment in which Alice and Bob measure the state of their qubits and try to violate Bell's inequality. This way we will be able to establish a threshold in visibility of the sources for the protocol to succeed.

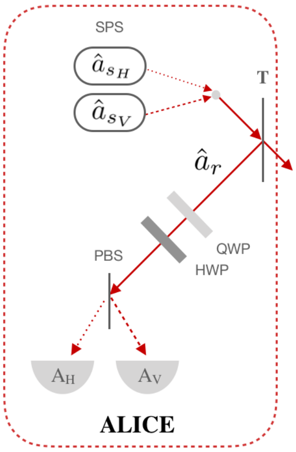

Figure 4.1: Detail from the main set-up, focused on Alice's station. Her measuring device consists of a Quarter-Wave Plate (QWP) and a Half-Wave Plate (HWP) followed by a polarizing beam splitter that directs the photon to the detector A_H if it is horizontally polarized or to A_V if it is vertically polarized. Bob has an identical measuring set-up.

4.2.1 The measuring devices

In the previous section the state of Alice and Bob's photons was evaluated using a density matrix representation. The way this state can be measured is by means of density matrix tomography, which was introduced in section 1.4. The way one can project the state in different ways on the Bloch sphere is by using two different waveplates (see Figure 4.1). The density matrix can be calculated in terms of the probabilities associated to measuring in diferent projective states. In an optical circuit, one can create these projective states by varying the angles of two consecutive QWP and HWP. The next step is to describe explicitly how they can reconstruct the state that they have my using such measurement device. The action of the waveplates on the creation operators of the photons is represented by the Jones matrices [43], which are described by unitary operations:

$$\hat{U}_{QWP}(\theta) = \frac{1}{\sqrt{2}}\begin{pmatrix} i-\cos(2\theta) & \sin(2\theta) \\ \sin(2\theta) & i+\cos(2\theta) \end{pmatrix}, \quad \hat{U}_{HWP}(\phi) = \begin{pmatrix} \cos(2\phi) & -\sin(2\phi) \\ -\sin(2\phi) & -\cos(2\phi) \end{pmatrix}. \tag{4.10}$$

As explained, these unitary transformations act on the creation operators of the photons right before they arrive to the measurement devices; that is, they act on $\hat{a}^\dagger_{H_{f1}}$, $\hat{a}^\dagger_{V_{f2}}$, $\hat{b}^\dagger_{H_{f3}}$ and $\hat{b}^\dagger_{f4}$ to transform them as

$$\begin{aligned} \hat{\mathbf{A}} \equiv \begin{pmatrix} \hat{A}_H \\ \hat{A}_V \end{pmatrix} = \hat{U}_{tot}(\theta_A, \phi_A)\begin{pmatrix} \hat{a}_{H_{f1}} \\ \hat{a}_{V_{f2}} \end{pmatrix} \equiv \hat{U}_{tot}(\theta_A, \phi_A)\hat{\mathbf{a}} \\ \hat{\mathbf{B}} \equiv \begin{pmatrix} \hat{B}_H \\ \hat{B}_V \end{pmatrix} = \hat{U}_{tot}(\theta_B, \phi_B)\begin{pmatrix} \hat{b}_{H_{f3}} \\ \hat{b}_{V_{f4}} \end{pmatrix} \equiv \hat{U}_{tot}(\theta_B, \phi_B)\hat{\mathbf{b}} \end{aligned}. \tag{4.11}$$

The operators $\hat{A}_i$ and $\hat{B}_i$ represent the measurement of photons at the corresponding detector (Figure 4.1) and $\hat{U}_{tot}$ is the total transformation associated to each set of waveplates, given by the product of the two consecutive unitary transformations:

$$\hat{U}_{tot}(\theta,\phi) = \hat{U}_{HWP}(\phi)\hat{U}_{QWP}(\theta) = \\ = \frac{1}{\sqrt{2}}\begin{pmatrix} \cos(2\phi)(i-\cos(2\theta)) - \sin(2\phi)\sin(2\theta) & -\sin(2\phi)(i+\cos(2\theta)) + \cos(2\phi)\sin(2\theta) \\ -\cos(2\phi)\sin(2\theta) - \sin(2\phi)(i-\cos(2\theta)) & -\sin(2\phi)\sin(2\theta) - \cos(2\phi)(i+\cos(2\theta)) \end{pmatrix}. \tag{4.12}$$

One can try to rewrite this transformation in order to get a more intuitive overview of its action on the Bloch sphere. We can do that by using the Stokes parameters, writing the transformation in the basis of the Pauli matrices using equation 1.31. We calculate the corresponding parameters S_i and obtain[3]:

$$\hat{U}_{tot}(\theta,\phi) = \frac{1}{\sqrt{2}}\left[-\cos 2(\phi-\theta)\mathbb{1} + i(-\sin 2\phi\hat{\sigma}_x - \sin 2(\phi-\theta)\hat{\sigma}_y + \cos 2\phi\hat{\sigma}_z)\right], \tag{4.13}$$

which is a more useful expression for the upcoming calculations. Then, with this transformation we can now relate the basis in which 4.8 is written to the detector basis.

4.2.2 The detection of photons

In order to proceed with the measurement we have to take one final step - to understand how the photodetection works (following [41]). The quantization of the electromagnetic field allows us to write the electric field operator, $\hat{E}(\mathbf{x},t) = \hat{E}^{(-)}(\mathbf{x},t) + \hat{E}^{(+)}(\mathbf{x},t)$, as

$$\hat{E}^{(+)}(\mathbf{x},t) \propto \hat{a}(t), \quad \hat{E}^{(-)}(\mathbf{x},t) \propto \hat{a}^\dagger(t), \tag{4.14}$$

where $\hat{E}^{(+)}(\mathbf{x},t)$ is the component of the field that describes absorption [9, p. 121]. The detection of a photon has to account for all the transitions from the initial state of the detector $|\psi_i\rangle$ (which can be the ground state of an atom, for example) to all possible final states $|\psi_f\rangle$. The probability of detection is, thus:

$$\begin{aligned}\sum_f |\langle\psi_f|\hat{E}^{(+)}(\mathbf{x},t)|\psi_i\rangle|^2 &= \sum_f \langle\psi_i|\hat{E}^{(-)}(\mathbf{x},t)|\psi_f\rangle\langle\psi_f|\hat{E}^{(+)}(\mathbf{x},t)|\psi_i\rangle \\ &= \langle\psi_i|\hat{E}^{(-)}(\mathbf{x},t)\hat{E}^{(+)}(\mathbf{x},t)|\psi_i\rangle \propto \langle\psi_i|\hat{a}^\dagger(t)\hat{a}(t)|\psi_i\rangle,\end{aligned} \tag{4.15}$$

where we have assumed a complete basis of final states $\sum_f |\psi_f\rangle\langle\psi_f| = \mathbb{1}$. As the probability of detection follows equation 4.15, it is reasonable to define a photodetection operator as $\hat{N} \equiv \hat{D}^\dagger\hat{D}$. If, furthermore, one wants to account for the number of photons that arrive at the detector during a certain integration time τ, then[4] [47, p. 70-73]:

$$\hat{N}(t,\tau) \equiv \int_t^{t+\tau} \hat{D}^\dagger(t')\hat{D}(t')dt' \tag{4.16}$$

The measurements that Alice and Bob will perform with their measurement devices respectively, will be the difference in number of counts of their pair of detectors whose clicks are created by the operators $\hat{A}_H$ and $\hat{A}_V$, and $\hat{B}_H$ and $\hat{B}_V$. Therefore, taking into account that in our case we consider

[3]Here we change the notation of the Introduction into the following one, more convenient in this section and the rest of the thesis: $\hat{\sigma}_0 \equiv \mathbb{1}$, $\hat{\sigma}_1 \equiv \hat{\sigma}_x$, $\hat{\sigma}_2 \equiv \hat{\sigma}_y$, $\hat{\sigma}_3 \equiv \hat{\sigma}_z$.

[4]In case it was desirable to account for the efficiency η_d of the detector itself, it suffices with modifying the expectation value of the photon detector operator as $\langle\hat{N}'\rangle = \eta_d\langle\hat{N}\rangle$ [47, p. 71].

an infinite integration time for simplicity, and using equation 4.16 we obtain the expression for the difference in counts operators $\hat{Q}_A$ and $\hat{Q}_B$:

$$\begin{aligned}\hat{Q}_A(t) &\equiv \hat{N}_{A_H}(t) - \hat{N}_{A_V}(t) = \int \hat{A}_H^\dagger(t)\hat{A}_H(t)dt - \int \hat{A}_V^\dagger(t)\hat{A}_V(t)dt,\\ \hat{Q}_B(t) &\equiv \hat{N}_{B_H}(t) - \hat{N}_{B_V}(t) = \int \hat{B}_H^\dagger(t)\hat{B}_H(t)dt - \int \hat{B}_V^\dagger(t)\hat{B}_V(t)dt\,,\end{aligned} \tag{4.17}$$

which can be written in terms of $\hat{\sigma}_z$ by using vector notation:

$$\begin{aligned}\hat{Q}_A(t) &= \iint \begin{pmatrix}\hat{A}_H^\dagger(t) & \hat{A}_V^\dagger(t')\end{pmatrix} \hat{\sigma}_z \begin{pmatrix}\hat{A}_H(t)\\ \hat{A}_V(t')\end{pmatrix} dtdt' = \iint \hat{\mathbf{A}}^\dagger(t,t')\hat{\sigma}_z\hat{\mathbf{A}}(t,t')dtdt',\\ \hat{Q}_B(t) &= \iint \begin{pmatrix}\hat{B}_H^\dagger(t) & \hat{B}_V^\dagger(t')\end{pmatrix} \hat{\sigma}_z \begin{pmatrix}\hat{B}_H(t)\\ \hat{B}_V(t')\end{pmatrix} dtdt' = \iint \hat{\mathbf{B}}^\dagger(t,t')\hat{\sigma}_z\hat{\mathbf{B}}(t,t')dtdt'\,,\end{aligned} \tag{4.18}$$

However, we would like to write the result in terms of the creation operators of the photons that arrive to the measuring devices, $\left\{\hat{a}_{H_{f1}}^\dagger, \hat{a}_{V_{f2}}^\dagger, \hat{b}_{H_{f3}}^\dagger, \hat{b}_{V_{f4}}^\dagger\right\}$, as it is the basis in which the state of the entangled pair is written. We can change to that basis by applying equation 4.11 to equation 4.18:

$$\begin{aligned}\hat{Q}_A(t) &= \iint \mathbf{a}^\dagger(t,t')\hat{U}_{tot}^\dagger(\theta_A,\phi_A)\hat{\sigma}_z\hat{U}_{tot}(\theta_A,\phi_A)\mathbf{a}(t,t')dtdt' \equiv \iint \mathbf{a}^\dagger(t,t')\hat{M}_A(\theta_A,\phi_A)\mathbf{a}(t,t')dtdt',\\ \hat{Q}_B(t) &= \iint \mathbf{b}^\dagger(t,t')\hat{U}_{tot}^\dagger(\theta_B,\phi_B)\hat{\sigma}_z\hat{U}_{tot}(\theta_B,\phi_B)\mathbf{b}(t,t')dtdt' \equiv \iint \mathbf{b}^\dagger(t,t')\hat{M}_B(\theta_B,\phi_B)\mathbf{b}(t,t')dtdt'\,,\end{aligned} \tag{4.19}$$

where we have defned the measurement operators $\hat{M}_A$ and $\hat{M}_B$ as:

$$\begin{aligned}\hat{M}_A(\theta_A,\phi_A) &\equiv \hat{U}_{tot}(\theta_A,\phi_A)^\dagger\hat{\sigma}_z\hat{U}_{tot}(\theta_A,\phi_A)\\ \hat{M}_B(\theta_B,\phi_B) &\equiv \hat{U}_{tot}(\theta_B,\phi_B)^\dagger\hat{\sigma}_z\hat{U}_{tot}(\theta_B,\phi_B)\end{aligned} \tag{4.20}$$

The measurement operators include all the action that is made by the measurement device: both the unitary transformation performed by the two waveplates and the difference in counts at the detectors. If we substitute equation 4.13 in the definition 4.20, one can see that $\hat{M}_A$ and $\hat{M}_B$ are again a combination of Pauli matrices, which can be written in the form:

$$\hat{M}_i = X_i\hat{\sigma}_x + Y_i\hat{\sigma}_y + Z_i\hat{\sigma}_z \tag{4.21}$$

where $i = A, B$ and normalization is satisfied ($X_i^2 + Y_i^2 + Z_i^2 = 1$). In other words, these measurement operators can be easily written in terms of coefficients that will help us understand better, their action on the Bloch sphere. By combining equations 4.13 and 4.20 and applying the trigonometric identities $\sin A \pm \sin B = 2\sin\frac{A\pm B}{2}\cos\frac{A\mp B}{2}$, $\cos A + \cos B = 2\cos\frac{A+B}{2}\cos\frac{A-B}{2}$ and $\cos A - \cos B = 2\sin\frac{A+B}{2}\sin\frac{A-B}{2}$, the coefficients X_i, Y_i, and Z_i are found to be:

$$\begin{cases} X_i &= -\sin 2\theta_i \cos 2(2\phi_i - \theta_i)\\ Y_i &= -\sin 2(2\phi_i - \theta_i)\\ Z_i &= \cos 2\theta_i \cos 2(2\phi_i - \theta_i)\end{cases} \tag{4.22}$$

One can find the inverse relation for equation 4.22, so it is possible to evaluate the angles corresponding to a given set of coefficients (which will be usefu later for optimisation over the coefficients):

$$\theta_i = -\frac{1}{2}\arctan\frac{X_i}{Z_i}, \quad \phi_i = -\frac{1}{4}(\arctan\frac{X_i}{Z_i} + \arcsin Y_i)\,. \tag{4.23}$$

We rewrite equation 4.22, to parametrize in terms of spherical coordinates:

$$\begin{cases} X_i &= \sin\xi_i \cos\gamma_i \\ Y_i &= \sin\xi_i \sin\gamma_i \\ Z_i &= \cos\xi_i \end{cases} \iff \begin{cases} \xi_i = \operatorname{acos}\left(\cos(-2\theta_i)\cos(-2(2\phi_i-\theta_i))\right) \\ \gamma_i = \operatorname{asin}\frac{\sin(-2(2\phi_i-\theta_i))}{\sqrt{1-\cos^2(-2\theta_i)\cos^2(-2(2\phi_i-\theta_i))}} \end{cases} \tag{4.24}$$

We have then fully characterised the measurement operators $\hat{M}_A$ and $\hat{M}_B$, in a more comprehensible way in the Pauli matrices basis. Moving forward, the total measurement operator of both systems $\hat{M} \equiv \hat{M}_A \otimes \hat{M}_B$ (with $\hat{M} = \hat{M}(\theta_A, \theta_B, \phi_A, \phi_B)$) can be calculated now explicitly by using the coefficients from equation 4.24 and the Stokes expression from 1.39:

$$\hat{M} = \frac{1}{4}\begin{pmatrix} S_{33} & S_{31}-iS_{32} & S_{13}-iS_{23} & S_{11}-iS_{12}-iS_{21}-S_{22} \\ S_{31}+iS_{32} & -S_{33} & S_{11}+iS_{12}-iS_{21}+S_{22} & -S_{13}+iS_{23} \\ S_{13}+iS_{23} & S_{11}-iS_{12}+iS_{21}+S_{22} & -S_{33} & -S_{31}+iS_{32} \\ S_{11}+iS_{12}+iS_{21}-S_{22} & -S_{13}-iS_{23} & -S_{31}-iS_{32} & S_{33} \end{pmatrix}, \tag{4.25}$$

where S_{ij} are calculated following equation 1.35 as $S_{ij} = S_i \otimes S_j$. Recall that, in terms of the coefficients in 4.21, $\frac{1}{2}S_1 = X$, $\frac{1}{2}S_2 = Y$ and $\frac{1}{2}S_3 = Z$. For example, the Stokes parameter S_{32} equals $S_{32} = S_3 \otimes S_2 = 4Z_A(\theta_A, \phi_A)Y_B(\theta_B, \phi_B)$. Note that $S_0 = 0$ both for Alice and Bob. This simplifies considerably the total measurement operator (equation 4.25). The purpose of writing $\hat{M}$ in the form of equation 4.25 is to have a more compact expression, compared to simply expanding the tensor product $\hat{M}_A \otimes \hat{M}_B$. Later we find that calculating the total difference in counts of the system is, thus, also more compact using the Stokes parameters. Furthermore, the measurement over the whole system, that is, the difference in counts for the total system, is given by the tensor product of both $\hat{Q}_T = \hat{Q}_A \otimes \hat{Q}_B$. Next, we expand it in terms of the measurement operators, using equation 4.19. In addition, we change index notation for the polarization, so we can pull the measurement operators out of the integrals and just leave inside the time-dependent operators:

$$\begin{aligned} \hat{Q}_T(t) = \hat{Q}_A(t) \otimes \hat{Q}_B(t) &= \iiiint \left(\mathbf{a}^\dagger(t,t')\hat{M}_A\mathbf{a}(t,t')\right) \otimes \left(\mathbf{b}^\dagger(t'',t''')\hat{M}_B\mathbf{b}(t'',t''')\right) dtdt'dt''dt''' \\ &= \sum_{ijkl}^{H,V} \iiiint \left(\hat{a}_i^\dagger(t)\hat{M}_{A_{ij}}\hat{a}_j(t')\right) \otimes \left(\hat{b}_k^\dagger(t'')\hat{M}_{B_{kl}}\hat{b}_l(t''')\right) dtdt'dt''dt''' \\ &= \sum_{ijkl}^{H,V} \left(\hat{M}_{A_{ij}} \otimes \hat{M}_{B_{kl}}\right) \iiiint \hat{a}_i^\dagger(t)\hat{a}_j(t')\hat{b}_k^\dagger(t'')\hat{b}_l(t''')dtdt'dt''dt''' \,. \end{aligned} \tag{4.26}$$

The expected value of the total difference in counts denoted by the operator $\hat{Q}_T$ is calculated by using the density matrix that we just calculated in equation 4.8. We get:

$$\begin{aligned} \left\langle \hat{Q}_T \right\rangle &= \mathrm{Tr}\left\{\hat{Q}_T\rho\right\} \\ &= \mathrm{Tr}\left\{\sum_{ijkl}^{H,V}\left(\hat{M}_{A_{ij}} \otimes \hat{M}_{B_{kl}}\right)\left(\iiiint \hat{a}_i^\dagger(t)\hat{a}_j(t')\hat{b}_k^\dagger(t'')\hat{b}_l(t''')dtdt'dt''dt''\right)\rho_{ijkl}\right\} \\ &\equiv \mathrm{Tr}\left\{\sum_{ijkl}^{H,V}(\hat{M}_{A_{ij}} \otimes \hat{M}_{B_{kl}})\rho'_{ijkl}\right\} = \mathrm{Tr}\left\{(\hat{M}_A \otimes \hat{M}_B)\rho'\right\}, \end{aligned} \tag{4.27}$$

where ρ' has been defined as the density matrix representing the state before the measurement but *without* any time dependence in it, as the time dependence left in the creation operators of the photons after the reflection at the first beam splitter is already integrated in $\iiiint \hat{a}_i^\dagger(t)\hat{a}_j(t')\hat{b}_k^\dagger(t'')\hat{b}_l(t''')$. In other words, redefining ρ as if it was already time independent before the measurement allows us to perform theoretically the measurement only via the angle-dependent operators $\hat{M}$ on a time-independent density matrix ρ'. In reality, the integration in time is carried, obviously, after photons are detected; however, acknowledging how the density matrix would have looked before the measurement in polarization provides us with a more complete picture of the entangled state shared by Alice and Bob, as well as a simplification of the measurement process itself. Following equation 4.27, the global difference in counts $\left\langle \hat{Q}_T \right\rangle$ depends simply on the expected value of the measurement operators of the systems $\mathrm{Tr}\left\{(\hat{M}_A \otimes \hat{M}_B)\rho'\right\}$. Let us calculate explicity the time-independent density matrix ρ'[5]:

$$\begin{aligned}
\left\langle \hat{Q}_T \right\rangle &= \mathrm{Tr}\left\{ \sum_{ijkl}^{H,V} \left(\hat{M}_{A_{ij}} \otimes \hat{M}_{B_{kl}}\right) \rho'_{ijkl} \right\} = \sum_{ijkl}^{H,V} \mathrm{Tr}\left\{ \left(\hat{M}_{A_{ij}} \otimes \hat{M}_{B_{kl}}\right) \rho'_{ijkl} \right\} \\
&= \frac{\eta^2 T^2 (1-T)^2}{4} \left(\mathrm{Tr}\left\{ \left(\hat{M}_{A_{HH}} \otimes \hat{M}_{B_{HH}}\right) \left(\iiiint \hat{a}_H^\dagger \hat{a}_H \hat{b}_H^\dagger \hat{b}_H \right) \rho_{HHHH} \right\} + ... \right) \\
&= \frac{\eta^2 T^2 (1-T)^2}{4} \cdot \\
&(\, \mathrm{Tr}\left\{ \left(\hat{M}_{A_{HH}} \otimes \hat{M}_{B_{HH}}\right) \left(\iiiint \hat{a}_H^\dagger \hat{a}_H \hat{b}_H^\dagger \hat{b}_H \right) (1-\beta^2) \hat{a}_{H_{f1}}^\dagger \hat{b}_{H_{f3}}^\dagger \left|\emptyset\right\rangle \left\langle\emptyset\right| \hat{a}_{H_{f1}} \hat{b}_{H_{f3}} \right\} \\
&+ \mathrm{Tr}\left\{ \left(\hat{M}_{A_{VH}} \otimes \hat{M}_{B_{VH}}\right) \left(\iiiint \hat{a}_V^\dagger \hat{a}_H \hat{b}_V^\dagger \hat{b}_H \right) (\beta^2-\alpha^2) \hat{a}_{H_{f1}}^\dagger \hat{b}_{H_{f3}}^\dagger \left|\emptyset\right\rangle \left\langle\emptyset\right| \hat{a}_{V_{f1}} \hat{b}_{V_{f3}} \right\} + ...) \,.
\end{aligned} \tag{4.28}$$

Now we can apply the cyclic property of the trace again, giving

$$\begin{aligned}
\left\langle \hat{Q}_T \right\rangle = \frac{\eta^2 T^2 (1-T)^2}{4} (\, &\mathrm{Tr}\left\{ \left(\hat{M}_{A_{HH}} \otimes \hat{M}_{B_{HH}}\right) (1-\beta^2) \left\langle \hat{a}_{H_{f1}} \hat{b}_{H_{f3}} (\iiiint \hat{a}_H^\dagger \hat{a}_H \hat{b}_H^\dagger \hat{b}_H) \hat{a}_{H_{f1}}^\dagger \hat{b}_{H_{f3}}^\dagger \right\rangle \right\} \\
&+ \mathrm{Tr}\left\{ \left(\hat{M}_{A_{VH}} \otimes \hat{M}_{B_{VH}}\right) (\beta^2-\alpha^2) \left\langle \hat{a}_{V_{f2}} \hat{b}_{V_{f4}} (\iiiint \hat{a}_V^\dagger \hat{a}_H \hat{b}_V^\dagger \hat{b}_H) \hat{a}_{H_{f1}}^\dagger \hat{b}_{H_{f3}}^\dagger \right\rangle \right\} + ...) \,.
\end{aligned} \tag{4.29}$$

Given that the creation operators from Alice and Bob commute, the expectation value can be rearranged as:

$$\begin{aligned}
\left\langle \hat{Q}_T \right\rangle &= \frac{\eta^2 T^2 (1-T)^2}{4} (\, \mathrm{Tr}\left\{ \left(\hat{M}_{A_{HH}} \otimes \hat{M}_{B_{HH}}\right) (1-\beta^2) \iiiint \left\langle \hat{a}_{H_{f1}} \hat{a}_H^\dagger \hat{a}_H \hat{a}_{H_{f1}}^\dagger \right\rangle \left\langle \hat{b}_{H_{f3}} \hat{b}_H^\dagger \hat{b}_H \hat{b}_{H_{f3}}^\dagger \right\rangle \right\} \\
&\qquad + \mathrm{Tr}\left\{ \left(\hat{M}_{A_{VH}} \otimes \hat{M}_{B_{VH}}\right) (\beta^2-\alpha^2) \iiiint \left\langle \hat{a}_{V_{f2}} \hat{a}_V^\dagger \hat{a}_H \hat{a}_{H_{f1}}^\dagger \right\rangle \left\langle \hat{b}_{V_{f4}} \hat{b}_V^\dagger \hat{b}_H \hat{b}_{H_{f3}}^\dagger \right\rangle \right\} + ...) \\
&= \frac{\eta^2 T^2 (1-T)^2}{4} (\, \mathrm{Tr}\left\{ \left(\hat{M}_{A_{HH}} \otimes \hat{M}_{B_{HH}}\right) (1-\beta^2) \cdot 1 \right\} + \mathrm{Tr}\left\{ \left(\hat{M}_{A_{VH}} \otimes \hat{M}_{B_{VH}}\right) (\beta^2-\alpha^2) \alpha^2 \right\} + ...) \,,
\end{aligned} \tag{4.30}$$

To calculate the expected values we have integrated in time and applied both the Dirac delta relation $\int \delta(a-x)\delta(x-b)dx = \delta(a-b)$ and the properties of creation operators discussed in the

[5]The time dependence has been ommitted in the integrals of the following equations to clarify the notation.

previous chapter. After integrating, the expected values proporcionate further combinations of overlapping $\langle f_i|f_j\rangle$ inner products in the density matrix of the state. Note that while expected values of the diagonal give 1, the expected values corresponding to the off-diagonal of ρ provide with extra α^2 terms. However, if we continue the calculation from here, the polarization dependence is also traced out, as we basically then trace over all the degrees of freedom. It was explained in the tomography section that, to figure out the density matrix before the measurement, we would need to reconstruct it by measuring a finite amount of times. Instead, in equation 4.30 we have the necessary ingredients to make a certain educated guess on how this time-independent density matrix would look like, by associating the coefficients we just found out in each element of the sum. This time-independent density matrix ρ' yields:

$$\rho' = \frac{{\eta_t}^2 T^2 (1-T)^2}{4} \begin{pmatrix} 1-\beta^2 & 0 & 0 & \alpha^2(\beta^2-\alpha^2) \\ 0 & 1+\beta^2 & -\alpha^2(\alpha^2+\beta^2) & 0 \\ 0 & -\alpha^2(\alpha^2+\beta^2) & 1+\beta^2 & 0 \\ \alpha^2(\beta^2-\alpha^2) & 0 & 0 & 1-\beta^2 \end{pmatrix}. \tag{4.31}$$

This matrix, unlike ρ, verifies that a statistical mixture is obtained when photons from the same station are completely distinguishable, $\alpha = 0$. This stronger bound on the distinguishability of photons coming from the same station than from the opposite is intuitive and only arises after all the time dependence that has been traced out from the state. We can now, finally, calculate the result of the measurement. The expected value for the difference in counts, measuring over ρ' and inserting the measurement operator written in terms of the Stokes parameters (equation 4.21):

$$\begin{aligned} \left\langle \hat{Q}_T \right\rangle &= \mathrm{Tr}\left\{ \hat{M}\rho' \right\} = \\ &= \frac{{\eta_t}^2 T^2 (1-T)^2}{16} \left(\left(1-\beta^2\right) S_{33} + \alpha^2\left(\beta^2-\alpha^2\right)\left(S_{11} - iS_{12} - iS_{21} - S_{22}\right) + \left(1+\beta^2\right)\left(-S_{33}\right) \right. \\ &- \alpha^2\left(\alpha^2+\beta^2\right)\left(S_{11} + iS_{12} - iS_{21} + S_{22}\right) - \alpha^2\left(\alpha^2+\beta^2\right)\left(S_{11} - iS_{12} + iS_{21} + S_{22}\right) \\ &+ \left. \left(1+\beta^2\right)\left(-S_{33}\right) + \alpha^2\left(\beta^2-\alpha^2\right)\left(S_{11} + iS_{12} + iS_{21} - S_{22}\right) + \left(1-\beta^2\right) S_{33} \right), \end{aligned} \tag{4.32}$$

which simplifying gives the final result:

$$\left\langle \hat{Q}_T \right\rangle = -\frac{\eta_t^2 T^2 (1-T)^2}{4} \left[\alpha^4 S_{11} + \alpha^2\beta^2 S_{22} + \beta^2 S_{33}\right]. \tag{4.33}$$

Finally, we write the result in the notation introduced for the coefficients of $\hat{M}$ (equation 4.25), giving:

$$\begin{aligned} \left\langle \hat{Q}_T \right\rangle = -\eta_t^2 T^2 (1-T)^2 [\alpha^4 X_A(\theta_A,\phi_A) X_B(\theta_B,\phi_B) + \alpha^2\beta^2 Y_A(\theta_A,\phi_A) Y_B(\theta_B,\phi_B) + \\ + \beta^2 Z_A(\theta_A,\phi_A) Z_B(\theta_B,\phi_B)]. \end{aligned} \tag{4.34}$$

As we can see, the outcome of the global measurement in difference in counts depends solely, up to normalization of the state, on the chosen angles of the two sets of HWP and QWP and on the distinguishability of photons. Therefore we can optimise the outcome of the measurement by choosing the appropiate measurement angles.

4.2.3 Violation of Bell's inequality

In the following we will calculate how the degree of distinguishability of the photons can affect the required violation of Bell's inequality during the protocol. The inequality that will be used is the

CHSH inequality [12]:

$$S = |C(\mathbf{a},\mathbf{b}) + C(\mathbf{a}',\mathbf{b}) + C(\mathbf{a},\mathbf{b}') - C(\mathbf{a}',\mathbf{b}')| \leq 2\,, \tag{4.35}$$

where $\mathbf{a},\mathbf{a}',\mathbf{b},\mathbf{b}'$ are unitary vectors along with the correlation C, that are measured as explained in the Introduction. The correlations used to calculate the inequality are the output of the final measurement (equation 4.34). Both Alice and Bob need two different sets of angles in their corresponding HWP and QWP. However, before calculating the correlations we have to normalize the total difference in counts. We do it by dividing equation 4.34 by the total number of counts $\left\langle \hat{N}_T \right\rangle$, which equals the probability of the two chosen events to occur: recall from Chapter 1 that this probability is $\eta_t^2 T^2(1-T)^2$ as only two of the total 8 possible events are considered valid. Looking at equation 4.18, it is easy to see that the total number of counts can be calculated with measurement operators that satisfy $\hat{M}_i = \mathbb{1}$. In fact, the total number of counts reduces to the trace of ρ':

$$\left\langle \hat{N}_T \right\rangle = \mathrm{Tr}\{(\mathbb{1}_A \otimes \mathbb{1}_B)\,\rho'\} = \mathrm{Tr}\{\rho'\} = \eta_t^2 T^2 (1-T)^2\,. \tag{4.36}$$

Thus the angle dependent correlation yields

$$C(\mathbf{a},\mathbf{b}) = -\left(\alpha^4 X_A(\theta_A,\phi_A)X_B(\theta_B,\phi_B) + \alpha^2\beta^2 Y_A(\theta_A,\phi_A)Y_B(\theta_B,\phi_B) + \beta^2 Z_A(\theta_A,\phi_A)Z_B(\theta_B,\phi_B)\right)\,. \tag{4.37}$$

We can then write all the correlations needed to construct the inequality. The angle dependence will be ommitted for simplicity, as well as the global minus sign, which becomes irrelevant inside the absolute value of the inequality:

$$\begin{aligned} C(\mathbf{a},\mathbf{b}) &= \alpha^4 X_A X_B + \alpha^2\beta^2 Y_A Y_B + \beta^2 Z_A Z_B,\\ C(\mathbf{a}',\mathbf{b}) &= \alpha^4 X'_A X_B + \alpha^2\beta^2 Y'_A Y_B + \beta^2 Z'_A Z_B,\\ C(\mathbf{a},\mathbf{b}') &= \alpha^4 X_A X'_B + \alpha^2\beta^2 Y_A Y'_B + \beta^2 Z_A Z'_B,\\ C(\mathbf{a}',\mathbf{b}') &= \alpha^4 X'_A X'_B + \alpha^2\beta^2 Y'_A Y'_B + \beta^2 Z'_A Z'_B\,. \end{aligned} \tag{4.38}$$

Recall that because of their normalization condition, $\{X_i, Y_i, Z_i\} \in [-1,1]$. The task now is to relate the visibility, and thus the distinguishability of the photons, to the violation of the inequality. It is important to note that the visibility of sources from the same lab (α) is assumed to be better than the one from opposite sides (β), meaning that $\alpha > \beta$. However, to begin with, we study a simpler limit in which $\alpha = \beta$. In Figure 4.2 left, S is represented in terms of the distinguishability after optimising over the parameters X_A, X'_A, Y_A, Y'_A, Z_A, Z'_A, X_B, X'_B, Y_B, Y'_B, Z_B and Z'_B for every value of distinguishability. The obtained result shows that for the protocol to succeed, a visibility of the sources of $\alpha = \beta \simeq 88\%$ is required. As a sanity check, note that for the indistinguishable case ($\alpha = \beta = 1$), the maximum violation of Bell's inequality $S = 2\sqrt{2}$) is achieved as expected. For the case when $\alpha \neq \beta$, a contour map has been plotted in Figure 4.2 right. The border between the green and orange section delimites the violation of the Bell inequality. It is observed that a potential distinguishability of photons from the same station being better than across stations (meaning $\alpha > \beta$) matches the result: for example, if a distinguishability of 90% can be reached by single photon sources from the same station, it is only required that they are distinguishable from photons coming from the other station in a 87%.

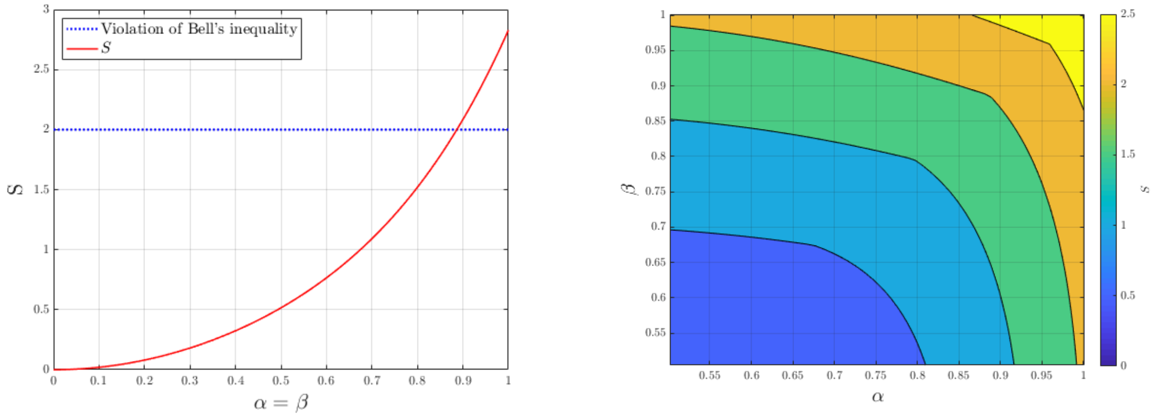

Figure 4.2: On the left, the CHSH violation parameter S is represented in terms of the distinguishability after optimising the angles for every value of α and β. A distinguishability of $\alpha = \beta \simeq 88\%$ is required for the protocol to succeed in this limit. On the right, contour map of the CHSH violation parameter as function of the distinguishability variables α and β. The measuring angles of the four HWQ and QWP have been optimized for every combination of distinguishabilities. The limit for the protocol to succeed is delimited by the border between the green and orange regions in the plot.

4.3 Visibility achieved with InGaAs quantum dots and conclusion

An important question to investigate is whether the single-photon sources that we want to work with, InGaAs quantum dots, can satisfy these conditions of visibility. In general, the reason why the visibility of the single photon sources is never completely perfect is due exclusively to the coupling of the quantum dot to phonons under resonant excitation [45]. In fact, this coupling creates decoherence within the decay time of the quantum dot and therefore the emmitted photons are not completely distinguishable. To answer properly to whether they would be able to satisfy the protocol, first of all we translate our results given in α and β to the visibility of the sources by using the result obtained in the previous chapter (equation 3.18):

$$V_\alpha = \alpha^2, \quad V_\beta = \beta^2 \,. \tag{4.39}$$

We can then plot our results in terms of the HOM visibilities V_α and V_β instead, which is shown in Figures 4.3 and 4.4. For equal visibilities, a minimum $V_\alpha = V_\beta \simeq 79\%$ is required. To place our results in context, note that already years ago HOM visibilities of 87% were reached by Spin-Flip Raman Transitions in quantum dots [48] and 67% for on-chip proposals [49]. More recently, almost complete indistinguishability has been accomplished experimentally using InGaAs quantum dots [50] [51]; in particular, a distinguishability of 94% has been reached at 4K [3], as well as 93% for distant qubits [52]. In conclusion, InGaAs quantum dots should be very much able to satisfy the visibility requirements of the protocol.

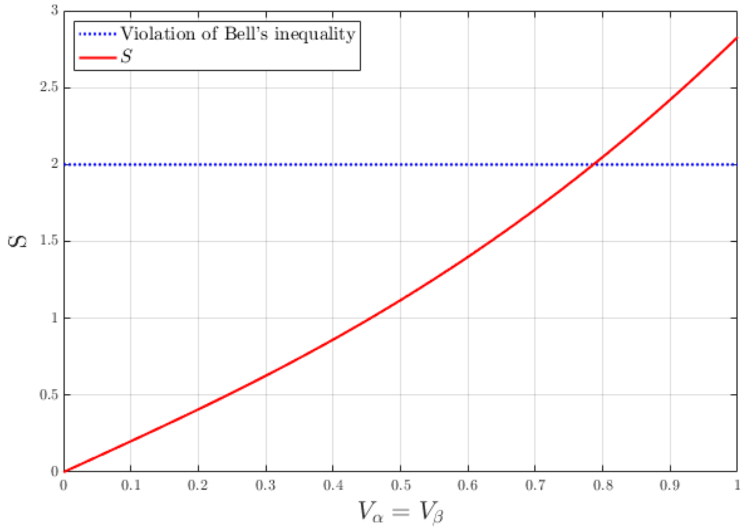

Figure 4.3: The combination of CHSH violation parameter S is represented in terms of the visibility after optimising the measurement angles. A visibility of $\alpha = \beta \simeq 79\%$ is required for the protocol to succeed in this limit.

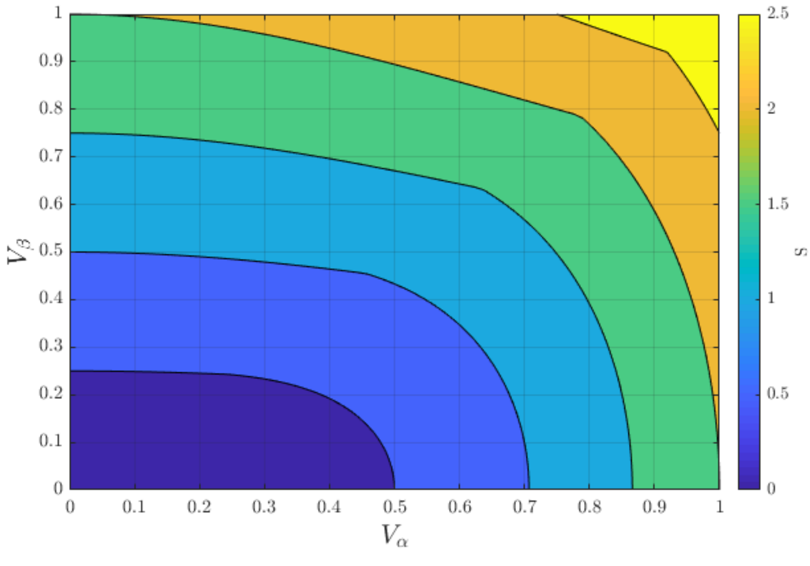

Figure 4.4: Contour map of the HOM visibility, giving the corresponding value of the CHSH inequality in the coloured z axis. The measuring angles of the four HWQ and QWP have been optimized for every combination of visibilities. The limit for the protocol to succeed is delimited by the border between the green and orange regions in the plot.

Chapter 5

Analysis of the effect of losses and multiphoton events

The central heralding station will tell Alice and Bob when two photons arrived and clicked in the correct combination. But does it mean that the protocol succeded? We described in Chapter 2 how photons can get lost at any point of the set-up, as well as the existence of multiphoton effects that disguise incorrect combinations of clicks as correct ones due to the incapacity of the detectors to measure how many photons arrived simultaneously. In this chapter, a thorough analysis of the protocol will be done by taking into account all kinds of losses, multiphoton detection errors, and the distinguishability of photons.

5.1 Introduction to the notation

The purpose of this chapter is, as mentioned above, to account for all the events that can be detected as correct by the heralding station. We will calculate the probability of each of them to happen, and thus we need to introduce a proper notation to label clearly each of them. We define the probability P_{ijkl} of each event as:

$$P_{ijkl} \quad \equiv \quad \begin{cases} i & \rightarrow \quad \text{number of photons that arrived to the CHS} \\ j & \rightarrow \quad \text{number of photons detected by Alice} \\ k & \rightarrow \quad \text{number of photons detected by Bob} \\ l & \rightarrow \quad \text{number of lost photons} \end{cases} \tag{5.1}$$

Note that in the above definition of probabilities we do not include events concerning more than one photon emission by the sources. Therefore, it is obvious that $i + j + k + l = 4$ must always be satisfied. Furthermore, $i \geq 2$ holds, as at least two photons must arrive to the heralding station to be able to produce a combination of clicks that the heralded station detects as valid. Let us consider an example. The heralding station sent a message to Alice and Bob, stating the reception of a correct event after two photons were detected simultaneously with orthogonal polarizations. Bob starts then to measure his part of the entangled state; however, Alice did not detect any photon associated to the event. How could this happen? There are two different possibilities, the first one being that corresponding to the term P_{2011}, which considers that one photon got lost. At the same time, this contribution can be generated by two different events. The lost photon could have been

Event probability	CHS	Alice	Bob	Lost photons
P_{2110}	AB	A	B	∅
P_{2200}	BB	AA	∅	∅
P_{2020}	AA	∅	BB	∅
P_{2101}	AB BB	A A	∅ ∅	B A
P_{2011}	AB AA	∅ ∅	B B	A B
P_{2002}	AB AA BB	∅ ∅ ∅	∅ ∅ ∅	AB BB AA
P_{3100}	ABB	A	∅	∅
P_{3010}	AAB	∅	B	∅
P_{3001}	ABB AAB	∅ ∅	∅ ∅	A B
P_{4000}	AABB	∅	∅	∅

Table 5.1: Description of all the different probabilities of events that lead to what the heralding station interprets as a correct generation of the entangled state. The notation used is defined in equation 5.1. The labels A and B describe where were the photons indicated by the notation P_{ijkl} generated. The header of columns assigns where the photons were detected.

generated by Alice if the two that clicked on the heraled station came from Alice and Bob stations respectively. In this case the photon got lost during the transmission within Alice's station. On the other hand, maybe both photons generated by Alice made it to the heralding station, and therefore it was one of Bob's photons that got lost. The other probability contribution is P_{3010}, that considers that no photon was lost at any point, but both photons generated by Alice arrived to the heralding station and created a correct combination of clicks together with Bob's transmitted photon in a way that the station could not identify as incorrect. Table 5.1 collects all the different possibilities that, similarly to the example just depicted, have one or more contributions from where the photons are generated and detected.

5.2 Analysis of events

We have all the necessary tools to calculate the probability of each projection. The way the probabilities are calculated, is a bit different to that in the previous chapter. In order to delimitate each event, the corresponding density matrix ρ_{ijkl} is calculated[1]. This density matrix will be written in the basis of the creation operators $\hat{a}^\dagger_{Hf1}, \hat{a}^\dagger_{Vf2}, \hat{b}^\dagger_{Hf3}, \hat{b}^\dagger_{Vf4}$. We will transform it into the basis of the detectors by applying the unitary transformation $\hat{U}_{tot}(\theta, \phi)$:

$$\rho'_{ijkl} = \hat{U}_{tot}(\theta, \phi)\rho_{ijkl}\hat{U}^\dagger_{tot}(\theta, \phi)\,. \tag{5.2}$$

[1]This is not the same matrix element ρ_{ijkl} from Chapter 3

On the other hand, the operators that represent a click occurring on either the detector A_H or A_V (B_H or B_V) are given by the identity minus the projection of vacuum on that detector. This way we ensure that we do not limit the projection of the incoming state:

$$\begin{aligned} \hat{M}_{+_A} &\equiv \mathbb{1} - \left|\emptyset\right\rangle \left\langle\emptyset\right|_{A_H}, \quad \hat{M}_{+_B} \equiv \mathbb{1} - \left|\emptyset\right\rangle \left\langle\emptyset\right|_{B_H}, \\ \hat{M}_{-_A} &\equiv \mathbb{1} - \left|\emptyset\right\rangle \left\langle\emptyset\right|_{A_V}, \quad \hat{M}_{-_B} \equiv \mathbb{1} - \left|\emptyset\right\rangle \left\langle\emptyset\right|_{B_V}. \end{aligned} \tag{5.3}$$

Therefore, the probability of a certain projection will be given by:

$$\begin{aligned} P_{ijkl_+} &= \mathrm{Tr}\Big\{\hat{M}_+ \rho'_{ijkl}\Big\} = \mathrm{Tr}\Big\{\hat{M}_+ \hat{U}_{tot}(\theta,\phi)\rho_{ijkl}\hat{U}^\dagger_{tot}(\theta,\phi)\Big\}, \\ P_{ijkl_-} &= \mathrm{Tr}\Big\{\hat{M}_- \rho'_{ijkl}\Big\} = \mathrm{Tr}\Big\{\hat{M}_- \hat{U}_{tot}(\theta,\phi)\rho_{ijkl}\hat{U}^\dagger_{tot}(\theta,\phi)\Big\}, \end{aligned} \tag{5.4}$$

where $\hat{M}_+ = \hat{M}_{+_A} \otimes \hat{M}_{+_B}$ and $\hat{M}_- = \hat{M}_{-_A} \otimes \hat{M}_{-_B}$. In the following subsections we will calculate the necessary ingredients to be able to complete the whole analysis of events.

5.2.1 Calculation of expectation values

In this subsection, we calculated all the necessary expectation values for the upcoming analysis. In Chapter 2, we explained how we choose the combination of operators at the heralding station that lead to the correct combinations of clicks. We do a similar task when calculating the expectation value of the operators $\hat{O}_{fi}$ (equation 4.3), that represent the creation of a photon at the heralding station. If two photons arrive at the heralding station from different preceeding stations (for example, the photons f_1 and f_3):

$$\begin{aligned} &\left\langle \hat{O}_{f1}\hat{O}_{f3}\hat{O}^\dagger_{f1}\hat{O}^\dagger_{f3}\right\rangle = \\ &< \left(-i\sqrt{1-t}(\hat{p}_{H_{f1}} + \hat{p}_{V_{f1}}) + \sqrt{t}(\hat{q}_{H_{f1}} + \hat{q}_{V_{f1}})\right)\left(\sqrt{t}(\hat{p}_{H_{f3}} + \hat{p}_{V_{f3}}) - i\sqrt{1-t}(\hat{q}_{H_{f3}} + \hat{q}_{V_{f3}})\right)\cdot \\ &\left(i\sqrt{1-t}(\hat{p}^\dagger_{H_{f1}} + \hat{p}^\dagger_{V_{f1}}) + \sqrt{t}(\hat{q}^\dagger_{H_{f1}} + \hat{q}^\dagger_{V_{f1}})\right)\left(\sqrt{t}(\hat{p}^\dagger_{H_{f3}} + \hat{p}^\dagger_{V_{f3}}) + i\sqrt{1-t}(\hat{q}^\dagger_{H_{f3}} + \hat{q}^\dagger_{V_{f3}})\right) > . \end{aligned} \tag{5.5}$$

Selecting only the combinations of operators that lead to a correct event, that is, D_1D_4 and D_2D_3 and applying the relations from section 2.1, we finally obtain:

$$\begin{aligned} \left\langle \hat{O}_{f1}\hat{O}_{f3}\hat{O}^\dagger_{f1}\hat{O}^\dagger_{f3}\right\rangle_{14,23} &=< \left(t\left(\hat{p}_{H_{f3}}\hat{q}_{H_{f1}} + \hat{p}_{V_{f3}}\hat{q}_{H_{f1}}\right) - (1-t)\left(\hat{p}_{H_{f1}}\hat{q}_{H_{f3}} + \hat{p}_{V_{f1}}\hat{q}_{H_{f3}}\right)\right)\cdot \\ &\left(t\left(\hat{p}^\dagger_{H_{f3}}\hat{q}^\dagger_{H_{f1}} + \hat{p}^\dagger_{V_{f3}}\hat{q}^\dagger_{H_{f1}}\right) - (1-t)\left(\hat{p}^\dagger_{H_{f1}}\hat{q}^\dagger_{H_{f3}} + \hat{p}^\dagger_{V_{f1}}\hat{q}^\dagger_{H_{f3}}\right)\right) > \\ &= 2\left(1 - 2t\left(1-t\right)\left(1+\beta^2_{13}\right)\right). \end{aligned} \tag{5.6}$$

Similarly, for the other combinations:

$$\begin{aligned} \left\langle \hat{O}_{f1}\hat{O}_{f4}\hat{O}^\dagger_{f1}\hat{O}^\dagger_{f4}\right\rangle_{14,23} &= 2\left(1 - 2t\left(1-t\right)\left(1-\beta^2_{14}\right)\right), \\ \left\langle \hat{O}_{f2}\hat{O}_{f3}\hat{O}^\dagger_{f2}\hat{O}^\dagger_{f3}\right\rangle_{14,23} &= 2\left(1 - 2t\left(1-t\right)\left(1-\beta^2_{23}\right)\right), \\ \left\langle \hat{O}_{f2}\hat{O}_{f4}\hat{O}^\dagger_{f2}\hat{O}^\dagger_{f4}\right\rangle_{14,23} &= 2\left(1 - 2t\left(1-t\right)\left(1+\beta^2_{24}\right)\right). \end{aligned} \tag{5.7}$$

On the contrary, if we do not postselect any event and accept all the combinations in order to do a sanity check, the expectation values are independent of the distinguishability of photons and the probability of transmission t of the central beam splitter and satisfy:

$$\left\langle \hat{O}_{f1}\hat{O}_{f3}\hat{O}^{\dagger}_{f1}\hat{O}^{\dagger}_{f3} \right\rangle = \left\langle \hat{O}_{f1}\hat{O}_{f4}\hat{O}^{\dagger}_{f1}\hat{O}^{\dagger}_{f4} \right\rangle = \left\langle \hat{O}_{f2}\hat{O}_{f3}\hat{O}^{\dagger}_{f2}\hat{O}^{\dagger}_{f3} \right\rangle = \left\langle \hat{O}_{f2}\hat{O}_{f4}\hat{O}^{\dagger}_{f2}\hat{O}^{\dagger}_{f4} \right\rangle = 4\,. \quad (5.8)$$

For completeness, we further obtain

$$\begin{aligned}
&\left\langle \hat{O}_{f1}\hat{O}_{f2}\hat{O}^{\dagger}_{f1}\hat{O}^{\dagger}_{f2} \right\rangle_{14,23} = 4t\,(1-t)\left(1-\alpha_{12}^2\right), \quad \left\langle \hat{O}_{f3}\hat{O}_{f4}\hat{O}^{\dagger}_{f3}\hat{O}^{\dagger}_{f4} \right\rangle_{14,23} = 4t\,(1-t)\left(1-\alpha_{34}^2\right), \\
&\left\langle \hat{O}_{f1}\hat{O}_{f4}\hat{O}^{\dagger}_{f2}\hat{O}^{\dagger}_{f3} \right\rangle_{14,23} = 2\left(-\alpha_{12}\alpha_{34} + 2t(1-t)(\alpha_{12}\alpha_{34} - \beta_{13}\beta_{24})\right), \\
&\left\langle \hat{O}_{f1}\hat{O}_{f3}\hat{O}^{\dagger}_{f2}\hat{O}^{\dagger}_{f4} \right\rangle_{14,23} = 2\left(-\alpha_{12}\alpha_{34} + 2t(1-t)(\alpha_{12}\alpha_{34} + \beta_{14}\beta_{23})\right),
\end{aligned} \quad (5.9)$$

which also satisfies $\left\langle \hat{O}_{f1}\hat{O}_{f2}\hat{O}^{\dagger}_{f1}\hat{O}^{\dagger}_{f2} \right\rangle = \left\langle \hat{O}_{f3}\hat{O}_{f4}\hat{O}^{\dagger}_{f3}\hat{O}^{\dagger}_{f4} \right\rangle = 4$, if no postselection of events is done. It can be checked that any other expectation value corresponding to the creation of two photons at the heralding station is equal to 0. Note that, on the other hand, for the indistinguishable case ($\alpha_{12} = \alpha_{34} = 1$), $\left\langle \hat{O}_{f1}\hat{O}_{f2}\hat{O}^{\dagger}_{f1}\hat{O}^{\dagger}_{f2} \right\rangle_{14,23}$ and $\left\langle \hat{O}_{f3}\hat{O}_{f4}\hat{O}^{\dagger}_{f3}\hat{O}^{\dagger}_{f4} \right\rangle_{14,23}$ equal 0 for any value of the probability of transmission t. This makes sense, as the click combinations that are considered as valid correspond to clicking at different PBS with orthogonal polarization. If the photons have been generated by Alice, for example, the following transformation applies after the fixed HWP in transmission between her station and the CHS:

$$\hat{a}^{\dagger}_{H_{f1}}\hat{a}^{\dagger}_{V_{f2}} \rightarrow (\hat{a}^{'\dagger}_{H_{f1}} + \hat{a}^{'\dagger}_{V_{f1}})(\hat{a}^{'\dagger}_{H_{f2}} - \hat{a}^{'\dagger}_{V_{f2}}) = \hat{a}^{'\dagger}_{H_{f1}}\hat{a}^{'\dagger}_{H_{f2}} - \hat{a}^{'\dagger}_{H_{f1}}\hat{a}^{'\dagger}_{V_{f2}} + \hat{a}^{'\dagger}_{V_{f1}}\hat{a}^{'\dagger}_{H_{f2}} - \hat{a}^{'\dagger}_{V_{f1}}\hat{a}^{'\dagger}_{V_{f2}}\,. \quad (5.10)$$

When the photons are indistinguishable, they bunch together after the waveplate ($\hat{a}^{\dagger}_{H_{f1}}\hat{a}^{\dagger}_{V_{f2}} \rightarrow \hat{a}^{'\dagger 2}_{H} - \hat{a}^{'\dagger 2}_{V}$), and therefore no D_1D_4 or D_2D_3 clicks can ever happen, leading to an expectation value of 0.

The calculation of the expectation values for the creation of three and four photons at the heralding station is far more complex. Not only does it involve big amount of terms, but also how the selection of valid terms of the transformation should be done. Recall that the way we account for triple counts on the CHS giving a false positive event is every time two of the three photons arrive to the same detector and, globally, that is identified as D_1D_4 or D_2D_3. When constructing the transformations now, the combinations of clicks that are kept are those which can be masked as desired clicks. The criteria, in essence, is still the same: simultaneous clicks with orthogonal polarizations on detectors belonging to different PBS. Therefore, we keep triple combinations such $\hat{p}^{\dagger}_{V_{f1}}\left(\hat{q}^{\dagger}_{H_{f3}}\hat{q}^{\dagger}_{H_{f4}}\right)$ or quadruple combinations as $\hat{p}^{\dagger}_{V_{f1}}\left(\hat{q}^{\dagger}_{H_{f2}}\hat{q}^{\dagger}_{H_{f3}}\hat{q}^{\dagger}_{H_{f4}}\right)$ or $\left(\hat{p}^{\dagger}_{V_{f1}}\hat{p}^{\dagger}_{V_{f2}}\right)\left(\hat{q}^{\dagger}_{H_{f3}}\hat{q}^{\dagger}_{H_{f4}}\right)$. This last combination in particular would be understood by the heralding station as a D_2D_3 one, due to the fact that the detectors can not notice that two photons arrived instead of one on each detector. We again apply the relations proven in section 2.1 and obtain:

$$
\begin{aligned}
&\left\langle \hat{O}_{f1}\hat{O}_{f3}\hat{O}_{f4}\hat{O}^\dagger_{f1}\hat{O}^\dagger_{f3}\hat{O}^\dagger_{f4}\right\rangle_{14,23} = \\
&= 2(1+\alpha_{34}^2)(t^3+(1-t)^3) + 2t(1-t)\left(2+\beta_{13}^2+\beta_{14}^2-2\alpha_{34}\left(\alpha_{34}+\beta_{13}\beta_{14}\right)+2\beta_{14}^2-2\beta_{13}^2\right), \\
&\left\langle \hat{O}_{f2}\hat{O}_{f3}\hat{O}_{f4}\hat{O}^\dagger_{f2}\hat{O}^\dagger_{f3}\hat{O}^\dagger_{f4}\right\rangle_{14,23} = \\
&= 2(1+\alpha_{34}^2)(t^3+(1-t)^3) + 2t(1-t)\left(2+\beta_{23}^2+\beta_{24}^2-2\alpha_{34}\left(\alpha_{34}+\beta_{23}\beta_{24}\right)-2\beta_{24}^2+2\beta_{23}^2\right), \\
&\left\langle \hat{O}_{f3}\hat{O}_{f1}\hat{O}_{f2}\hat{O}^\dagger_{f3}\hat{O}^\dagger_{f1}\hat{O}^\dagger_{f2}\right\rangle_{14,23} = \\
&= 2(1+\alpha_{12}^2)(t^3+(1-t)^3) + 2t(1-t)\left(2+\beta_{13}^2+\beta_{23}^2-2\alpha_{12}\left(\alpha_{12}+\beta_{13}\beta_{23}\right)+2\beta_{23}^2-2\beta_{13}^2\right), \\
&\left\langle \hat{O}_{f4}\hat{O}_{f1}\hat{O}_{f2}\hat{O}^\dagger_{f4}\hat{O}^\dagger_{f1}\hat{O}^\dagger_{f2}\right\rangle_{14,23} = \\
&= 2(1+\alpha_{12}^2)(t^3+(1-t)^3) + 2t(1-t)\left(2+\beta_{14}^2+\beta_{24}^2-2\alpha_{12}\left(\alpha_{12}+\beta_{14}\beta_{24}\right)-2\beta_{24}^2+2\beta_{14}^2\right).
\end{aligned} \tag{5.11}
$$

As a sanity check, we calculate again the same expectation values but without excluding any term of the transformation this time. In fact, the expectation values are again independent of the distinguishability of photons and the transmittance t:

$$
\begin{aligned}
\left\langle \hat{O}_{f1}\hat{O}_{f3}\hat{O}_{f4}\hat{O}^\dagger_{f1}\hat{O}^\dagger_{f3}\hat{O}^\dagger_{f4}\right\rangle &= \left\langle \hat{O}_{f2}\hat{O}_{f3}\hat{O}_{f4}\hat{O}^\dagger_{f2}\hat{O}^\dagger_{f3}\hat{O}^\dagger_{f4}\right\rangle \\
&= \left\langle \hat{O}_{f3}\hat{O}_{f1}\hat{O}_{f2}\hat{O}^\dagger_{f3}\hat{O}^\dagger_{f1}\hat{O}^\dagger_{f2}\right\rangle = \left\langle \hat{O}_{f4}\hat{O}_{f1}\hat{O}_{f2}\hat{O}^\dagger_{f4}\hat{O}^\dagger_{f1}\hat{O}^\dagger_{f2}\right\rangle = 8\,.
\end{aligned} \tag{5.12}
$$

On the other hand, note that any other combination of operators, such $\left\langle \hat{O}_{f1}\hat{O}_{f3}\hat{O}_{f4}\hat{O}^\dagger_{f2}\hat{O}^\dagger_{f3}\hat{O}^\dagger_{f4}\right\rangle_{14,23}$, equals 0. Finally, for the (unlikely) case in which four photons arrive to the heralding station and click in a correct combination:

$$
\begin{aligned}
&\left\langle \hat{O}_{f1}\hat{O}_{f2}\hat{O}_{f3}\hat{O}_{f4}\hat{O}^\dagger_{f1}\hat{O}^\dagger_{f2}\hat{O}^\dagger_{f3}\hat{O}^\dagger_{f4}\right\rangle_{14,23} = 2(t^4+(1-t)^4)(1+\alpha_{12}^2)(1+\alpha_{34}^2) \\
&+ 4t^2(1-t)^2(2-\beta_{13}^2-\beta_{24}^2+3\beta_{23}^2+3\beta_{14}^2+\beta_{13}^2\beta_{24}^2+7\beta_{23}^2\beta_{14}^2-2\alpha_{12}^2-2\alpha_{34}^2-4\alpha_{12}\beta_{13}\beta_{23} \\
&- 2\alpha_{34}(\beta_{13}\beta_{14}+\beta_{23}\beta_{24})-2\beta_{13}\beta_{14}\beta_{23}\beta_{24}+2\alpha_{12}^2\alpha_{34}^2-2\beta_{13}^2\beta_{14}\beta_{24}+5\alpha_{12}\alpha_{34}\beta_{14}\beta_{23}-2\alpha_{12}\alpha_{34}\beta_{13}\beta_{24}) \\
&+ 4(t(1-t)^3+t^3(1-t))(\alpha_{12}^2+\alpha_{34}^2+2\beta_{14}^2+2\beta_{23}^2+\alpha_{34}(\beta_{13}\beta_{14}+\beta_{23}\beta_{24})+\alpha_{12}(\beta_{13}\beta_{23}+\beta_{14}\beta_{24}) \\
&+ 2\alpha_{12}\alpha_{34}(\beta_{14}\beta_{23}-\beta_{13}\beta_{24}))\,.
\end{aligned} \tag{5.13}
$$

5.2.2 Projection of events

We have already studied how the HWP and QWP perform a transformation on the polarization of the reflected photons at Alice and Bob's stations (subsection 1.2.3 in Chapter 3). In fact, equation 4.13 showed how the total transformation looks like in the Pauli matrices' basis. This resulted to be a very useful basis in order to define the difference in counts operator and the measurement operator $\hat{M}(\theta,\phi)$. In this chapter, however, we are interested in studying the click on one or the other detector separately, and thus we will describe the transformation slightly differently in order to clarify the notation. Expanding equation 4.13 in a single matrix form:

$$
\hat{U}_{tot}(\theta,\phi) = \frac{1}{\sqrt{2}}\begin{pmatrix} -\cos 2(\phi-\theta)+i\cos 2\phi & -\sin 2(\phi-\theta)-i\sin 2\phi \\ \sin 2(\phi-\theta)-i\sin 2\phi & -\cos 2(\phi-\theta)-i\cos 2\phi \end{pmatrix} \equiv \begin{pmatrix} U_{11} & U_{12} \\ U_{21} & U_{22} \end{pmatrix}. \tag{5.14}
$$

If we define the following expressions:

$$\Lambda \equiv \frac{1}{2}\left(\cos 2(\phi-\theta)^2+\cos 2\phi^2\right), \quad K \equiv \frac{1}{2}\left(\sin 2(\phi-\theta)^2+\sin 2\phi^2\right), \tag{5.15}$$

it holds that

$$|U_{11}|^2=|U_{22}|^2=U_{11}U_{22}=U_{11}^*U_{22}^*=\Lambda, \quad |U_{12}|^2=|U_{21}|^2=-U_{12}U_{21}=-U_{12}^*U_{21}^*=K\,. \tag{5.16}$$

Note that in fact $\Lambda + K = 1$ as expected. Furthermore, we define:

$$\begin{aligned}
\Gamma_{++} &\equiv \frac{1}{2}\left(i\sin 2(2\phi-\theta)+\sin 2\theta\cos 2(2\phi-\theta)\right), \quad \Gamma_{--} \equiv \frac{1}{2}\left(-i\sin 2(2\phi-\theta)-\sin 2\theta\cos 2(2\phi-\theta)\right),\\
\Gamma_{+-} &\equiv \frac{1}{2}\left(i\sin 2(2\phi-\theta)-\sin 2\theta\cos 2(2\phi-\theta)\right), \quad \Gamma_{-+} \equiv \frac{1}{2}\left(-i\sin 2(2\phi-\theta)+\sin 2\theta\cos 2(2\phi-\theta)\right),
\end{aligned} \tag{5.17}$$

which satisfies $\Gamma_{++}+\Gamma_{--}=\Gamma_{+-}+\Gamma_{-+}=0$ and allow to write in a compact way the following useful relations:

$$U_{11}U_{12}^*=\Gamma_{--}, \quad U_{12}U_{11}^*=\Gamma_{+-}, \quad U_{21}U_{22}^*=\Gamma_{++}, \quad U_{22}U_{21}^*=\Gamma_{-+}\,. \tag{5.18}$$

Finally, for the following calculations, recall that from equation 4.11 it holds that:

$$\begin{aligned}
&\begin{cases}\hat{a}_{H_{f1}}=U_{11_A}^*\hat{A}_{H_{f1}}+U_{21_A}^*\hat{A}_{V_{f1}}\\ \hat{a}_{V_{f2}}=U_{12_A}^*\hat{A}_{H_{f2}}+U_{22_A}^*\hat{A}_{V_{f2}}\end{cases} \qquad
\begin{cases}\hat{a}_{H_{f1}}^\dagger=U_{11_A}\hat{A}_{H_{f1}}^\dagger+U_{21_A}\hat{A}_{V_{f1}}^\dagger\\ \hat{a}_{V_{f2}}^\dagger=U_{12_A}\hat{A}_{H_{f2}}^\dagger+U_{22_A}\hat{A}_{V_{f2}}^\dagger\end{cases}\\
&\begin{cases}\hat{b}_{H_{f1}}=U_{11_B}^*\hat{B}_{H_{f1}}+U_{21_B}^*\hat{B}_{V_{f1}}\\ \hat{b}_{V_{f2}}=U_{12_B}^*\hat{B}_{H_{f2}}+U_{22_B}^*\hat{B}_{V_{f2}}\end{cases} \qquad
\begin{cases}\hat{b}_{H_{f1}}^\dagger=U_{11_B}\hat{B}_{H_{f1}}^\dagger+U_{21_B}\hat{B}_{V_{f1}}^\dagger\\ \hat{b}_{V_{f2}}^\dagger=U_{12_B}\hat{B}_{H_{f2}}^\dagger+U_{22_B}\hat{B}_{V_{f2}}^\dagger\end{cases}
\end{aligned} \tag{5.19}$$

We shall then proceed with the calculation of all the terms that conform Table 5.1. Let us start with a term which we have already detailed in Chapter 3, P_{2110}; however, losses where not included back then, so it will be a good example on how the calculations are carried out. First of all, we write the corresponding transformation to the event looking at equation 3.27. Two photons reach the heralding station while one is detected at Alice and Bob's stations respectively. No photon is lost so we drop the loss operators, obtaining

$$\begin{aligned}
\hat{a}_{H_{f1}}^\dagger &\to \sqrt{\frac{\eta_{1_{f1}}\eta_t T}{2}}\hat{O}_{f1}^\dagger + i\sqrt{\eta_{1_{f1}}\eta_{2_{f1}}(1-T)}\hat{a}_{H_{f1}}^\dagger,\\
\hat{a}_{V_{f2}}^\dagger &\to \sqrt{\frac{\eta_{1_{f2}}\eta_t T}{2}}\hat{O}_{f2}^\dagger + i\sqrt{\eta_{1_{f2}}\eta_{2_{f2}}(1-T)}\hat{a}_{V_{f2}}^\dagger,\\
\hat{b}_{H_{f3}}^\dagger &\to \sqrt{\frac{\eta_{1_{f3}}\eta_t T}{2}}\hat{O}_{f3}^\dagger + i\sqrt{\eta_{1_{f3}}\eta_{2_{f3}}(1-T)}\hat{b}_{H_{f3}}^\dagger,\\
\hat{b}_{V_{f4}}^\dagger &\to \sqrt{\frac{\eta_{1_{f4}}\eta_t T}{2}}\hat{O}_{f4}^\dagger + i\sqrt{\eta_{1_{f4}}\eta_{2_{f4}}(1-T)}\hat{b}_{V_{f4}}^\dagger,
\end{aligned} \tag{5.20}$$

and we restrict the operators to satisfy:

$$\begin{aligned}
\hat{a}_{H_{f1}}^\dagger\hat{a}_{V_{f2}}^\dagger &\to i\sqrt{\frac{\eta_{1_{f1}}\eta_{1_{f2}}\eta_t T(1-T)}{2}}\left(\sqrt{\eta_{2_{f2}}}\hat{O}_{f1}^\dagger\hat{a}_{V_{f2}}^\dagger+\sqrt{\eta_{2_{f1}}}\hat{O}_{f2}^\dagger\hat{a}_{H_{f1}}^\dagger\right),\\
\hat{b}_{H_{f3}}^\dagger\hat{b}_{V_{f4}}^\dagger &\to i\sqrt{\frac{\eta_{1_{f3}}\eta_{1_{f4}}\eta_t T(1-T)}{2}}\left(\sqrt{\eta_{2_{f4}}}\hat{O}_{f3}^\dagger\hat{b}_{V_{f4}}^\dagger+\sqrt{\eta_{2_{f3}}}\hat{O}_{f4}^\dagger\hat{b}_{H_{f3}}^\dagger\right).
\end{aligned} \tag{5.21}$$

These transformations allow us to calculate the density matrix ρ_{2110}. Then, applying equations 5.2 and 5.4, the projections over the detectors are calculated to be:

$$\begin{aligned}
P_{2110_{++}} = \mathrm{Tr}\Big\{\left(\hat{M}_{+_A}\otimes\hat{M}_{+_B}\right)\rho'_{2110}\Big\} = \frac{\eta_t^2 T^2(1-T)^2}{4}\eta_{1_{f1}}\eta_{1_{f2}}\eta_{1_{f3}}\eta_{1_{f4}}\cdot \\
[\eta_{2_{f1}}\eta_{2_{f3}}\left\langle\hat{O}_{f2}\hat{O}_{f4}\hat{O}^{\dagger}_{f2}\hat{O}^{\dagger}_{f4}\right\rangle\Lambda_A\Lambda_B + \eta_{2_{f1}}\eta_{2_{f4}}\left\langle\hat{O}_{f2}\hat{O}_{f3}\hat{O}^{\dagger}_{f2}\hat{O}^{\dagger}_{f3}\right\rangle\Lambda_A K_B + \\
+\eta_{2_{f2}}\eta_{2_{f3}}\left\langle\hat{O}_{f1}\hat{O}_{f4}\hat{O}^{\dagger}_{f1}\hat{O}^{\dagger}_{f4}\right\rangle K_A\Lambda_B + \eta_{2_{f2}}\eta_{2_{f4}}\left\langle\hat{O}_{f1}\hat{O}_{f3}\hat{O}^{\dagger}_{f1}\hat{O}^{\dagger}_{f3}\right\rangle K_A K_B + \\
+\sqrt{\eta_{2_{f1}}\eta_{2_{f2}}\eta_{2_{f1}}\eta_{2_{f4}}}\alpha_{12}\alpha_{34}\left\langle\hat{O}_{f1}\hat{O}_{f3}\hat{O}^{\dagger}_{f2}\hat{O}^{\dagger}_{f4}\right\rangle\left(\Gamma_{--_A}\Gamma_{--_B}+\Gamma_{+-_A}\Gamma_{+-_B}\right) + \\
+\sqrt{\eta_{2_{f1}}\eta_{2_{f2}}\eta_{2_{f1}}\eta_{2_{f4}}}\alpha_{12}\alpha_{34}\left\langle\hat{O}_{f1}\hat{O}_{f4}\hat{O}^{\dagger}_{f2}\hat{O}^{\dagger}_{f3}\right\rangle\left(\Gamma_{+-_A}\Gamma_{--_B}+\Gamma_{--_A}\Gamma_{+-_B}\right)]
\end{aligned} \tag{5.22}$$

$$\begin{aligned}
P_{2110_{+-}} = \mathrm{Tr}\Big\{\left(\hat{M}_{+_A}\otimes\hat{M}_{-_B}\right)\rho'_{2110}\Big\} = \frac{\eta_t^2 T^2(1-T)^2}{4}\eta_{1_{f1}}\eta_{1_{f2}}\eta_{1_{f3}}\eta_{1_{f4}}\cdot \\
[\eta_{2_{f1}}\eta_{2_{f3}}\left\langle\hat{O}_{f2}\hat{O}_{f4}\hat{O}^{\dagger}_{f2}\hat{O}^{\dagger}_{f4}\right\rangle\Lambda_A K_B + \eta_{2_{f1}}\eta_{2_{f4}}\left\langle\hat{O}_{f2}\hat{O}_{f3}\hat{O}^{\dagger}_{f2}\hat{O}^{\dagger}_{f3}\right\rangle\Lambda_A\Lambda_B + \\
+\eta_{2_{f2}}\eta_{2_{f3}}\left\langle\hat{O}_{f1}\hat{O}_{f4}\hat{O}^{\dagger}_{f1}\hat{O}^{\dagger}_{f4}\right\rangle K_A K_B + \eta_{2_{f2}}\eta_{2_{f4}}\left\langle\hat{O}_{f1}\hat{O}_{f3}\hat{O}^{\dagger}_{f1}\hat{O}^{\dagger}_{f3}\right\rangle K_A\Lambda_B + \\
+\sqrt{\eta_{2_{f1}}\eta_{2_{f2}}\eta_{2_{f1}}\eta_{2_{f4}}}\alpha_{12}\alpha_{34}\left\langle\hat{O}_{f1}\hat{O}_{f3}\hat{O}^{\dagger}_{f2}\hat{O}^{\dagger}_{f4}\right\rangle\left(\Gamma_{--_A}\Gamma_{++_B}+\Gamma_{+-_A}\Gamma_{-+_B}\right) + \\
+\sqrt{\eta_{2_{f1}}\eta_{2_{f2}}\eta_{2_{f1}}\eta_{2_{f4}}}\alpha_{12}\alpha_{34}\left\langle\hat{O}_{f1}\hat{O}_{f4}\hat{O}^{\dagger}_{f2}\hat{O}^{\dagger}_{f3}\right\rangle\left(\Gamma_{+-_A}\Gamma_{++_B}+\Gamma_{--_A}\Gamma_{-+_B}\right)]
\end{aligned} \tag{5.23}$$

$$\begin{aligned}
P_{2110_{-+}} = \mathrm{Tr}\Big\{\left(\hat{M}_{-_A}\otimes\hat{M}_{-_B}\right)\rho'_{2110}\Big\} = \frac{\eta_t^2 T^2(1-T)^2}{4}\eta_{1_{f1}}\eta_{1_{f2}}\eta_{1_{f3}}\eta_{1_{f4}}\cdot \\
[\eta_{2_{f1}}\eta_{2_{f3}}\left\langle\hat{O}_{f2}\hat{O}_{f4}\hat{O}^{\dagger}_{f2}\hat{O}^{\dagger}_{f4}\right\rangle K_A\Lambda_B + \eta_{2_{f1}}\eta_{2_{f4}}\left\langle\hat{O}_{f2}\hat{O}_{f3}\hat{O}^{\dagger}_{f2}\hat{O}^{\dagger}_{f3}\right\rangle K_A K_B + \\
+\eta_{2_{f2}}\eta_{2_{f3}}\left\langle\hat{O}_{f1}\hat{O}_{f4}\hat{O}^{\dagger}_{f1}\hat{O}^{\dagger}_{f4}\right\rangle\Lambda_A\Lambda_B + \eta_{2_{f2}}\eta_{2_{f4}}\left\langle\hat{O}_{f1}\hat{O}_{f3}\hat{O}^{\dagger}_{f1}\hat{O}^{\dagger}_{f3}\right\rangle\Lambda_A K_B + \\
+\sqrt{\eta_{2_{f1}}\eta_{2_{f2}}\eta_{2_{f1}}\eta_{2_{f4}}}\alpha_{12}\alpha_{34}\left\langle\hat{O}_{f1}\hat{O}_{f3}\hat{O}^{\dagger}_{f2}\hat{O}^{\dagger}_{f4}\right\rangle\left(\Gamma_{++_A}\Gamma_{--_B}+\Gamma_{-+_A}\Gamma_{+-_B}\right) + \\
+\sqrt{\eta_{2_{f1}}\eta_{2_{f2}}\eta_{2_{f1}}\eta_{2_{f4}}}\alpha_{12}\alpha_{34}\left\langle\hat{O}_{f1}\hat{O}_{f4}\hat{O}^{\dagger}_{f2}\hat{O}^{\dagger}_{f3}\right\rangle\left(\Gamma_{-+_A}\Gamma_{--_B}+\Gamma_{++_A}\Gamma_{+-_B}\right)]
\end{aligned} \tag{5.24}$$

$$\begin{aligned}
P_{2110_{--}} = \mathrm{Tr}\Big\{\left(\hat{M}_{-_A}\otimes\hat{M}_{-_B}\right)\rho'_{2110}\Big\} = \frac{\eta_t^2 T^2(1-T)^2}{4}\eta_{1_{f1}}\eta_{1_{f2}}\eta_{1_{f3}}\eta_{1_{f4}}\cdot \\
[\eta_{2_{f1}}\eta_{2_{f3}}\left\langle\hat{O}_{f2}\hat{O}_{f4}\hat{O}^{\dagger}_{f2}\hat{O}^{\dagger}_{f4}\right\rangle K_A K_B + \eta_{2_{f1}}\eta_{2_{f4}}\left\langle\hat{O}_{f2}\hat{O}_{f3}\hat{O}^{\dagger}_{f2}\hat{O}^{\dagger}_{f3}\right\rangle K_A A_B + \\
+\eta_{2_{f2}}\eta_{2_{f3}}\left\langle\hat{O}_{f1}\hat{O}_{f4}\hat{O}^{\dagger}_{f1}\hat{O}^{\dagger}_{f4}\right\rangle\Lambda_A K_B + \eta_{2_{f2}}\eta_{2_{f4}}\left\langle\hat{O}_{f1}\hat{O}_{f3}\hat{O}^{\dagger}_{f1}\hat{O}^{\dagger}_{f3}\right\rangle\Lambda_A\Lambda_B + \\
+\sqrt{\eta_{2_{f1}}\eta_{2_{f2}}\eta_{2_{f1}}\eta_{2_{f4}}}\alpha_{12}\alpha_{34}\left\langle\hat{O}_{f1}\hat{O}_{f3}\hat{O}^{\dagger}_{f2}\hat{O}^{\dagger}_{f4}\right\rangle\left(\Gamma_{++_A}\Gamma_{++_B}+\Gamma_{-+_A}\Gamma_{-+_B}\right) + \\
+\sqrt{\eta_{2_{f1}}\eta_{2_{f2}}\eta_{2_{f1}}\eta_{2_{f4}}}\alpha_{12}\alpha_{34}\left\langle\hat{O}_{f1}\hat{O}_{f4}\hat{O}^{\dagger}_{f2}\hat{O}^{\dagger}_{f3}\right\rangle\left(\Gamma_{-+_A}\Gamma_{++_B}+\Gamma_{++_A}\Gamma_{-+_B}\right)]
\end{aligned} \tag{5.25}$$

In fact, the total probability P_{2110} equals the sum over all the projections:

$$\begin{aligned}
P_{2110} = P_{2110_{++}} + P_{2110_{+-}} + P_{2110_{-+}} + P_{2110_{--}} = \frac{\eta_t^2 T^2(1-T)^2}{4}\eta_{1_{f1}}\eta_{1_{f2}}\eta_{1_{f3}}\eta_{1_{f4}}\cdot \\
[\eta_{2_{f1}}\eta_{2_{f3}}\left\langle\hat{O}_{f2}\hat{O}_{f4}\hat{O}^{\dagger}_{f2}\hat{O}^{\dagger}_{f4}\right\rangle + \eta_{2_{f1}}\eta_{2_{f4}}\left\langle\hat{O}_{f2}\hat{O}_{f3}\hat{O}^{\dagger}_{f2}\hat{O}^{\dagger}_{f3}\right\rangle + \\
+\eta_{2_{f2}}\eta_{2_{f3}}\left\langle\hat{O}_{f1}\hat{O}_{f4}\hat{O}^{\dagger}_{f1}\hat{O}^{\dagger}_{f4}\right\rangle + \eta_{2_{f2}}\eta_{2_{f4}}\left\langle\hat{O}_{f1}\hat{O}_{f3}\hat{O}^{\dagger}_{f1}\hat{O}^{\dagger}_{f3}\right\rangle].
\end{aligned} \tag{5.26}$$

To double check the result, we can take the limit in which the local efficiency is 1, as well as equal distinguishabilities α and β. If we substitute the expectation values of the photon operators at the heralding station by the corresponding to the succesful combinations D_1D_4/D_2D_3, we obtain the same probability as in Chapter 3, $\eta_t^2T^2(1-T)^2$. If on the contrary, we accept all combinations at the CHS, all the expectation values of the creation operators of photons at the heralding station are independent of any parameter equallying 4 (equation 5.8) thus obtaining the total probability $4\eta_t^2T^2(1-T)^2$. The rest of the detailed results for all the other probability contributions can be found in the Appendix A. However, we detail one specific case: the events P_{2200} and P_{2020}. These events share a special characteristic, compared to the others, as two photons arrive at the measurement devices of either Alice or Bob. In case two photons are indeed detected, there is no difficulty in identifying this event as incorrect and disregard it. However, as it was explained before, if both photons click simultaneously on the same detector, not Alice nor Bob would be able to tell the difference. This implies that we should stablish two different categories within these events: the probability that the two photons will click on the same ($P_{2200_{SD}}$ and $P_{2020_{SD}}$) or on different detectors ($P_{2200_{DD}}$ and $P_{2020_{DD}}$) . Whether they do or not will depend, of course, on the set of angles chosen for the HWP and QWP.

Let us start with P_{2200}. As the two photons generated by Alice stay in the station and it is the two photons generated by Bob arriving to the heralding station, the applied transformation yields:

$$\begin{aligned} \hat{a}^\dagger_{Hf1} &\to i\sqrt{\eta_{1_{f1}}\eta_{2_{f1}}(1-T)}\hat{a}^\dagger_{Hf1}, \quad \hat{b}^\dagger_{Hf3} \to \sqrt{\frac{\eta_{1_{f3}}\eta_t T}{2}}\hat{O}^\dagger_{f3}, \\ \hat{a}^\dagger_{Vf2} &\to i\sqrt{\eta_{1_{f2}}\eta_{2_{f2}}(1-T)}\hat{a}^\dagger_{Vf2}, \quad \hat{b}^\dagger_{Vf4} \to \sqrt{\frac{\eta_{1_{f4}}\eta_t T}{2}}\hat{O}^\dagger_{f4}, \end{aligned} \tag{5.27}$$

giving:

$$\begin{aligned} \hat{a}^\dagger_{Hf1}\hat{a}^\dagger_{Vf2} &\to -(1-T)\sqrt{\eta_{1_{f1}}\eta_{1_{f2}}\eta_{2_{f1}}\eta_{2_{f2}}}\hat{a}^\dagger_{Hf1}\hat{a}^\dagger_{V_2} \\ \hat{b}^\dagger_{Hf3}\hat{b}^\dagger_{Vf4} &\to \frac{\eta_t T}{2}\sqrt{\eta_{1_{f3}}\eta_{1_{f4}}}\hat{O}^\dagger_{f3}\hat{O}^\dagger_{f4}. \end{aligned} \tag{5.28}$$

Thus the associated density matrix:

$$\rho_{2200} = \frac{\eta_t^2T^2(1-T)^2}{4}\eta_{1_{f1}}\eta_{1_{f2}}\eta_{1_{f3}}\eta_{1_{f4}}\eta_{2_{f1}}\eta_{2_{f2}}\left\langle \hat{O}_{f3}\hat{O}_{f4}\hat{O}^\dagger_{f3}\hat{O}^\dagger_{f4}\right\rangle \left(\hat{a}^\dagger_{Hf1}\hat{a}^\dagger_{Vf2}\left|\emptyset\right\rangle\left\langle\emptyset\right|\hat{a}_{Hf1}\hat{a}_{Vf2}\right). \tag{5.29}$$

After applying the transformations associated to the HWP and QWP to ρ_{2200} and taking the trace, we keep terms contributing to the probability of clicks at the same detector $P_{2200_{SD}}$ the ones that go as $\left\langle \hat{A}_{Hf1}\hat{A}_{Hf2}\hat{A}^\dagger_{Hf1}\hat{A}^\dagger_{Hf2}\right\rangle = \left\langle \hat{A}_{Vf1}\hat{A}_{Vf2}\hat{A}^\dagger_{Vf1}\hat{A}^\dagger_{Vf2}\right\rangle = 1+\alpha_{12}^2$. On the contrary, the mixed terms $\left\langle \hat{A}_{Hf1}\hat{A}_{Vf2}\hat{A}^\dagger_{Hf1}\hat{A}^\dagger_{Vf2}\right\rangle = \left\langle \hat{A}_{Vf1}\hat{A}_{Hf2}\hat{A}^\dagger_{Vf1}\hat{A}^\dagger_{Hf2}\right\rangle = 1$ and $\left\langle \hat{A}_{Hf1}\hat{A}_{Vf2}\hat{A}^\dagger_{Vf1}\hat{A}^\dagger_{Hf2}\right\rangle = \left\langle \hat{A}_{Vf1}\hat{A}_{Hf2}\hat{A}^\dagger_{Hf1}\hat{A}^\dagger_{Vf2}\right\rangle = \alpha_{12}^2$ contribute to $P_{2200_{DD}}$, giving the results:

$$\begin{aligned} P_{2200_{SD+}} &= P_{2200_{SD-}} \\ &= \frac{\eta_t^2T^2(1-T)^2}{4}\eta_{1_{f1}}\eta_{1_{f2}}\eta_{1_{f3}}\eta_{1_{f4}}\eta_{2_{f1}}\eta_{2_{f2}}\left\langle \hat{O}_{f3}\hat{O}_{f4}\hat{O}^\dagger_{f3}\hat{O}^\dagger_{f4}\right\rangle(1+\alpha_{12}^2)\Lambda_A K_A, \\ P_{2200_{DD}} &= \\ &= \frac{\eta_t^2T^2(1-T)^2}{4}\eta_{1_{f1}}\eta_{1_{f2}}\eta_{1_{f3}}\eta_{1_{f4}}\eta_{2_{f1}}\eta_{2_{f2}}\left\langle \hat{O}_{f3}\hat{O}_{f4}\hat{O}^\dagger_{f3}\hat{O}^\dagger_{f4}\right\rangle\left(\Lambda_A^2+K_A^2-2\Lambda_A K_A\alpha_{12}^2\right), \end{aligned} \tag{5.30}$$

It is trivial to check that, in fact, the angle dependence goes away when calculating the whole term P_{2200}:

$$P_{2200} = P_{2200_{SD+}} + P_{2200_{SD-}} + P_{2200_{DD}} = \frac{\eta_t^2 T^2 (1-T)^2}{4} \eta_{1_{f1}} \eta_{1_{f2}} \eta_{1_{f3}} \eta_{1_{f4}} \eta_{2_{f1}} \eta_{2_{f2}} \left\langle \hat{O}_{f3} \hat{O}_{f4} \hat{O}^{\dagger}_{f3} \hat{O}^{\dagger}_{f4} \right\rangle . \tag{5.31}$$

The rest of the contributions depicted in Table 5.1 can be found in Appendix A.

5.3 Calculation of thresholds for the success of the protocol

Now that we have accounted for all the different extra events that can lead to a wrong message from the heralding station we can construct the Bell's inequality again. To begin with, we should clasify all the different possibilities in a bigger picture. Let us change a little bit the notation and define $P(A = i, B = j)$ as the joint probability for Alice to perform a measurement with outcome $i = \{+, -, \emptyset\}$ and for Bob with outcome $j = \{+, -, \emptyset\}$. As in the previous section, $+$ means that a clicked was measured on detectors A_H/B_H, whereas $-$ means that a clicked was measured on detectors A_V/B_V. If the outcome is $\emptyset$, then no photon was detected. In other words, $P(A = i, B = j)$ gives the probability for Alice and Bob to measure a photon, $P(A = i, B = \emptyset)$ and $P(A = \emptyset, B = j)$ gives the probability for one of them to measure a photon and the other not receive any and $P(A = \emptyset, B = \emptyset)$ gives the probability that both Alice and Bob performed no measurement at the detectors. Each of the different probability events specified in Table 5.1 contributes to one of these four terms, as detailed in Table 5.2. Note that the probability $P(A = \emptyset, B = \emptyset)$ will also account for all those events that are actually disregardable: $P_{2200_{DD}}$ and $P_{2020_{DD}}$. Recall that these two probabilities represent the simultaneous click on two detectors from the same local station, in which case is automatically identified as a wrong event. It is not the case for $P_{2200_{SD}}$ and $P_{2020_{SD}}$, which are interpreted as a single click, and thus contribute to $P(A = i, B = \emptyset)$ and $P(A = \emptyset, B = j)$, respectively. In Figure 5.1 we have plotted the different contributions to the probability of acceptance of the heralding station, $P(A = i, B = j)$[2], $P(A = i, B = \emptyset)$, $P(A = \emptyset, B = j)$ and $P(A = \emptyset, B = \emptyset)$, in terms of the probability of transmission of the first beam splitter, T (recall that T influences directly on the local efficiency, given that $\eta_l = \eta_1 \eta_2 (1 - T)$). The total heralding rate is calculated as the sum of all the contributions. For simplicity, we stay in a low transmission limit, $\eta_t \approx 0$, and with a 50:50 beam splitter placed at the heralding station. We can then study how much each of the probability contributions matter compared with each other depending on the distinguishability of the photons involved. It is important to understand why one should stay in a low T limit by looking at the plots shown in Figure 5.1: the bigger the transmission of the first beam splitter is, the better the heralding rate, *but* on the contrary the contribution of $P(A = i, B = \emptyset)$, $P(A = \emptyset, B = j)$ and $P(A = \emptyset, B = \emptyset)$ is higher and eventually bigger that the main probability term. When this happens, we start identifying as correct more failed events than correct ones, thus inserting a lot of noise in the protocol. For greater asymmetry and lower distinguishability, the margin of increase in T becomes less in order to gain a better heralding rate.

In the following we establish a way to relate the violation of Bell's inequality with the required efficiencies and distinguishability of photons. We have to decide a strategy for Alice and Bob to follow every time they do not measure a photon if we want to perform DIQKD. We will choose the

[2] We do not adopt any strategy of identification in this plot. $P(A = i, B = j)$ is basically identified solely with the term P_{2110}.

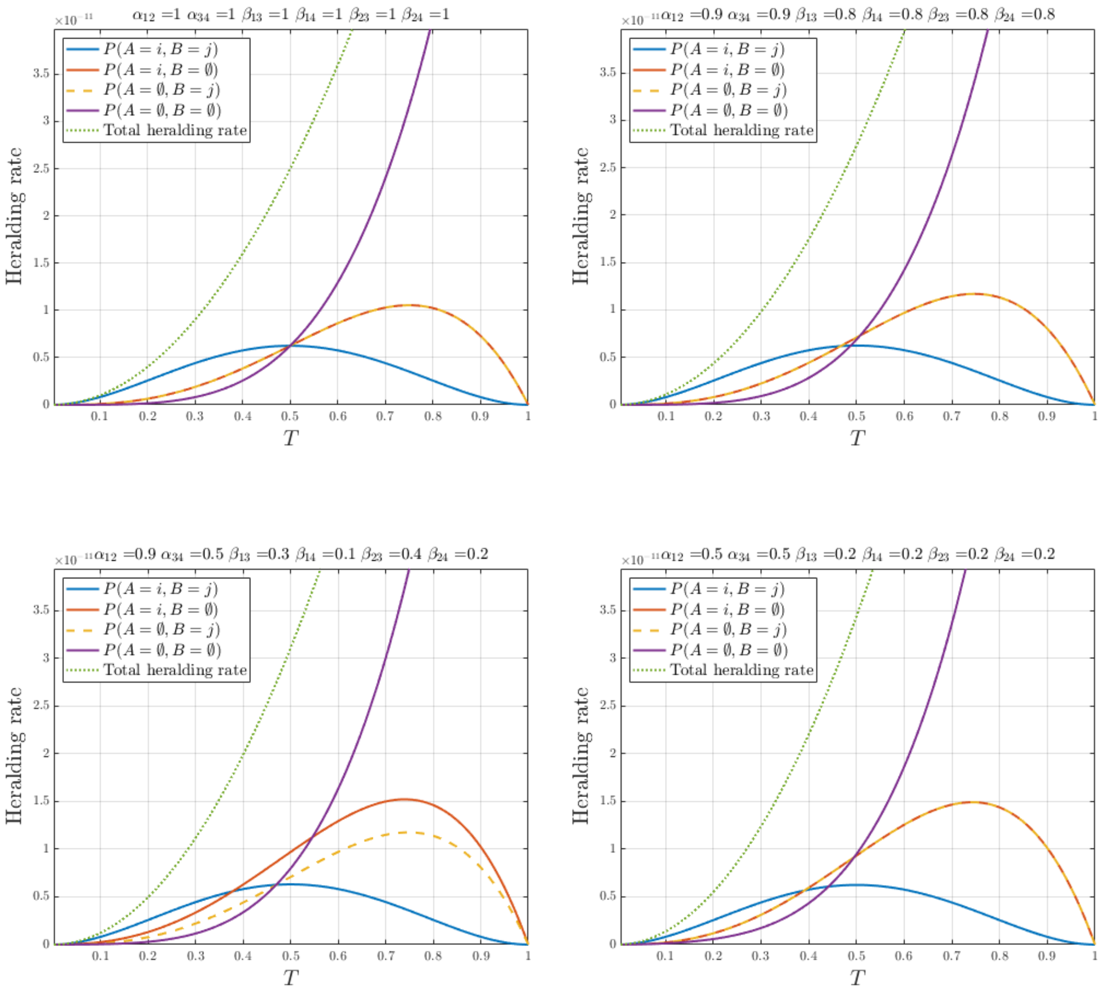

Figure 5.1: Heralding rate of the protocol and its different components in a low transmission limit, $\eta_t \approx 0.1$, and with a 50:50 beam splitter placed at the heralding station for several values of distinguishability of photons. As the distinguishability and asymmetry between photons from Alice and Bob's stations increase, the probability of incorrect events that are detected as approved by the heralding station increase at lower T. This implies that a bigger asymmetry regarding the distinguishability of photons forces to stay in a lower heralding rate regime in order to keep the dominance of the probability of correct events, $P(A = i, B = j)$.

$P(A=i,B=j)$	$P(A=i,B=\emptyset)$	$P(A=\emptyset,B=j)$	$P(A=\emptyset,B=\emptyset)$
P_{2110}	$P_{2200_{SD}}$	$P_{2020_{SD}}$	P_{2002}
	P_{2101}	P_{2011}	P_{3001}
	P_{3100}	P_{3010}	P_{4000}
			$P_{2200_{DD}}$
			$P_{2020_{DD}}$

Table 5.2: Distribution of all the different contributions to the probabilities $P(A=i,B=j)$, $P(A=i,B=\emptyset)$, $P(A=\emptyset,B=j)$ and $P(A=\emptyset,B=\emptyset)$.

one that is, at first sight, the simplest one: Alice and Bob will note as $i,j=+$ every time they do not get a click at the detector. In other words, we redefine the probability of Alice and Bob for obtaining i,j outcomes as $\tilde{P}(A=i,B=j)$, which satisfies:

$$\begin{aligned}\tilde{P}(A=i,B=j)=&P(A=i,B=j)+\delta_{j,+}P(A=i,B=\emptyset)+\delta_{i,+}P(A=\emptyset,B=j)\\&+\delta_{i,+}\delta_{j,+}P(A=\emptyset,B=\emptyset)\,.\end{aligned}\tag{5.32}$$

For more clarity, let us expand equation 5.32:

$$\begin{aligned}&\tilde{P}(A=-,B=-)=P(A=-,B=-),\\&\tilde{P}(A=+,B=-)=P(A=+,B=-)+P(A=\emptyset,B=-),\\&\tilde{P}(A=-,B=+)=P(A=-,B=+)+P(A=-,B=\emptyset),\\&\tilde{P}(A=+,B=+)=P(A=+,B=+)+P(A=+,B=\emptyset)+P(A=\emptyset,B=+)+P(A=\emptyset,B=\emptyset)\,,\end{aligned}\tag{5.33}$$

which, writing explicitly all the contributions attending to Table 5.1:

$$\begin{aligned}\tilde{P}(A=-,B=-)=&\quad P_{2110_{--}}\,,\\\tilde{P}(A=+,B=-)=&\quad P_{2110_{+-}}+P_{2011_{-}}+P_{3010_{-}}+P_{2020_{SD_{-}}}\,,\\\tilde{P}(A=-,B=+)=&\quad P_{2110_{-+}}+P_{2101_{-}}+P_{3100_{-}}+P_{2200_{SD_{-}}}\,,\\\tilde{P}(A=+,B=+)=&\quad P_{2110_{++}}+P_{2011_{+}}+P_{3010_{+}}+P_{2020_{SD_{+}}}+P_{2101_{+}}+P_{3100_{+}}+P_{2200_{SD_{+}}}\\&+P_{2002}+P_{3001}+P_{4000}+P_{2200_{DD}}+P_{2020_{DD}}\,.\end{aligned}\tag{5.34}$$

In Chapter 3, we constructed the correlations $C(\mathbf{a},\mathbf{b})$ that conform the CHSH inequality with the normalized difference in counts between the two detectors in each station, that was defined as the expectation value $\left\langle\hat{Q}_T\right\rangle$ (equation 4.37). However, in this chapter we have projected all the probabilities individually on each detector. In other words, we need to rewrite the expectation value of the difference in counts in terms of the probabilities $P(A=i,B=j)$, $P(A=i,B=\emptyset)$, $P(A=\emptyset,B=j)$ and $P(A=\emptyset,B=\emptyset)$. From equation 4.27 and taking into account the definitions from equation 5.3:

$$\begin{aligned}\left\langle\hat{Q}_T\right\rangle&=\mathrm{Tr}\left\{\hat{Q}_T\rho\right\}=\mathrm{Tr}\left\{\left(\hat{M}_A\otimes\hat{M}_B\right)\rho\right\}=\mathrm{Tr}\left\{\left(\hat{U}^{\dagger}_{tot}\left(\hat{M}_{+_A}-\hat{M}_{-_A}\right)\otimes\left(\hat{M}_{+_B}-\hat{M}_{-_B}\right)\hat{U}_{tot}\right)\rho\right\}\\&=\mathrm{Tr}\left\{\left(\hat{M}_{+_A}-\hat{M}_{-_A}\right)\otimes\left(\hat{M}_{+_B}-\hat{M}_{-_B}\right)\hat{U}_{tot}\rho\hat{U}^{\dagger}_{tot}\right\}\,,\end{aligned}\tag{5.35}$$

which leads to:

$$\begin{aligned}\left\langle \hat{Q}_T \right\rangle &= \mathrm{Tr}\left\{\left(\hat{M}_{+_A} \otimes \hat{M}_{+_B}\right)\rho'\right\} - \mathrm{Tr}\left\{\left(\hat{M}_{+_A} \otimes \hat{M}_{-_B}\right)\rho'\right\} \\ &- \mathrm{Tr}\left\{\left(\hat{M}_{-_A} \otimes \hat{M}_{+_B}\right)\rho'\right\} + \mathrm{Tr}\left\{\left(\hat{M}_{-_A} \otimes \hat{M}_{-_B}\right)\rho'\right\} \\ &= P(A=+,B=+) - P(A=+,B=-) - P(A=-,B=+) + P(A=-,B=-)\,. \end{aligned} \tag{5.36}$$

However, before calculating the correlations $C(\mathbf{a}, \mathbf{b})$ we have to normalize the total difference in counts, as we did in Chapter 3. Again, we must divide $\left\langle \hat{Q}_T \right\rangle$ by the total number of counts, which in this case is equivalent to the sum of all the different probability contributions from Table 5.1. To prove it more carefully, it is enough to calculate the total number of counts $\left\langle \hat{N}_T \right\rangle$ with measurement operators that satisfy $\hat{M}_i = \mathbb{1}$. In fact:

$$\begin{aligned}\left\langle \hat{N}_T \right\rangle &= \mathrm{Tr}\{(\mathbb{1}_A \otimes \mathbb{1}_B)\,\rho\} = \mathrm{Tr}\left\{\left(\hat{M}_{+_A} + \hat{M}_{-_A}\right) \otimes \left(\hat{M}_{+_B} + \hat{M}_{-_B}\right)\rho'\right\} \\ &= \mathrm{Tr}\left\{\left(\hat{M}_{+_A} \otimes \hat{M}_{+_B}\right)\rho'\right\} + \mathrm{Tr}\left\{\left(\hat{M}_{+_A} \otimes \hat{M}_{-_B}\right)\rho'\right\} \\ &+ \mathrm{Tr}\left\{\left(\hat{M}_{-_A} \otimes \hat{M}_{+_B}\right)\rho'\right\} + \mathrm{Tr}\left\{\left(\hat{M}_{-_A} \otimes \hat{M}_{-_B}\right)\rho'\right\} \\ &= P(A=+,B=+) + P(A=+,B=-) + P(A=-,B=+) + P(A=-,B=-)\,. \end{aligned} \tag{5.37}$$

Note that if we substitute equation 5.34 in equation 5.37, we indeed obtain that the total number of counts equals the sum of all the different probability contributions, which is obviously angle independent:

$$\left\langle \hat{N}_T \right\rangle = P_{2110} + P_{2011} + P_{3010} + P_{2020} + P_{2101} + P_{3100} + P_{2200} + P_{2002} + P_{3001} + P_{4000}\,. \tag{5.38}$$

Dividing the expression obtained for the expectation value of the total difference in counts by the total number of counts, this is, equation 5.36 by equation 5.37, we obtain the expression for the correlations $C(\mathbf{a}, \mathbf{b})$ in terms of the projected probabilities:

$$C(\mathbf{a}, \mathbf{b}) = \frac{P(A=+,B=+) - P(A=+,B=-) - P(A=-,B=+) + P(A=-,B=-)}{P(A=+,B=+) + P(A=+,B=-) + P(A=-,B=+) + P(A=-,B=-)}\,. \tag{5.39}$$

This way of constructing the correlation for a experimental realization of the violation of the CHSH inequality was introduced for the first time by the Bell test that Aspect realized in 1982 [14]. It is of course dependent on the measurement angles, but also on the transmission of the beam splitters involved, the distinguishability of photons and the transmission and local efficiencies. Ideally, the correlation reaches the extremes of the interval in which it is defined, $[-1, 1]$. However, due to the different errors we have introduced the correlation can not achieve ± 1, which is shown in Figure 5.2. In this plot, we have fixed all the HWP and QWP angles except for one, so we can study the relative evolution of the correlation based on one of them. In particular, θ_A varies from 0 tp π while we fix $\theta_B = -\pi/4$, $\phi_A = \pi/8$ and $\phi_B = \pi/2$. The reason to choose this combination in particular is that, it is one of the many combinations that allow $C(\mathbf{a}, \mathbf{b})$ to become ± 1, when considering only the angle dependence. In this example, we are in the indistinguishable photons limit, as well as establishing $T \approx 0$ and $t = 1/2$. By disminishing the local efficiency η_l we can appreciate how the correlation is unable to reach its maximum anymore, as it happened due to the

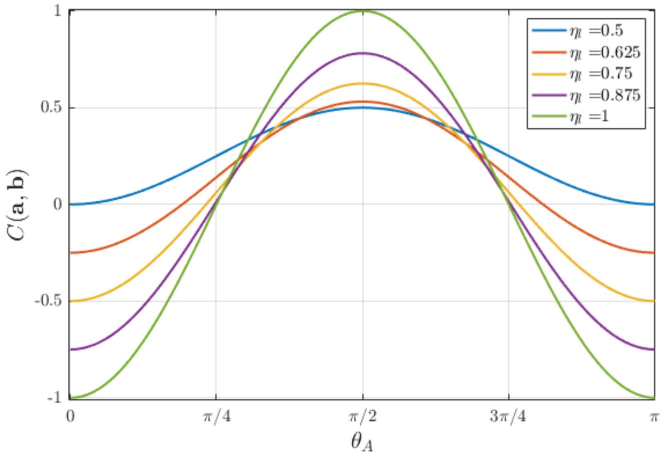

Figure 5.2: Correlation of the measurements realized by Alice and Bob in terms of the relative angle θ_A for several values of local efficiency η_l, after fixing the rest of them as $\theta_B = -\pi/4$, $\phi_A = \pi/8$ and $\phi_B = \pi/2$. The experiment is performed with indistinguishable photons and in the limit $T \approx 0$, with a 50:50 beam splitter in the heralding station.

non-ideal polarizers in [14]. We can already have an intuition on the effect that the local efficiency will have on the violation of the Bell inequality, given how it restricts each of the correlations.

5.3.1 Distinguishability and local efficiency

Once we have constructed the correlations $C(\mathbf{a}, \mathbf{b})$ (equation 5.39) we can proceed with analysing how the violation of the CHSH inequality is conditioned by not only the degree of distinguishability of photons as we studied in Chapter 3, but also the efficiency of the set-up and the influence of multiphoton events. Let us recall once more the CHSH inequality [12]:

$$S = |C(\mathbf{a}, \mathbf{b}) + C(\mathbf{a}', \mathbf{b}) + C(\mathbf{a}, \mathbf{b}') - C(\mathbf{a}', \mathbf{b}')| \leq 2 \tag{5.40}$$

Unlike in Chapter 3, whether S will satisfy $S \geq 2$ depends on all the new parameters that we have introduced in this chapter: not only the visibility of the sources, but also the local efficiencies $\eta_{1_{fi}}$, $\eta_{2_{fi}}$ (represented in the total local efficiency $\eta_l = \eta_1\eta_2(1-T)$) and the efficiency in transmission to the heralding station η_t. Note that it will also depend on the transmission of the first beam splitter T: due to all the additional events we take into account, T no longer goes away with the normalization of the correlation. The purpose of this subsection is to establish a threshold both in distinguishability and local efficiency upon which the CHSH inequality violation is satisfied. Let us start by assuming symmetry in the distinguishability of photons by claiming that $\alpha_{ij} = \alpha = \beta_{ij} = \beta$, as well as $\eta_{1_{fi}} = \eta_1$, $\eta_{2_{fi}} = \eta_2$, so that the number of parameters can be reduced and the results can be simplified. We have seen in Figure 5.1 how an asymmetry in distinguishability would only make the succes of the protocol harder. Furthermore, we will stay in the limit of low transmission $T \approx 0$, $\eta_t \approx 0$. This way we can also ensure that the probability of detecting false correct events at the heralding station is less comparable to P_{2110}, if we consider the graph in Figure 5.1. After setting this context for the parameters we construct the CHSH inequality optimizing S by means of the eight different angles for each value of distinguishability and local efficiency. The result is plot in Figure 5.3. We can see that the violation of the inequality occurs in two different areas of the plot: when the local efficiency is 0 for any value of the distinguishability of photons, and for both high local efficiency and indistinguishability. The first region is definitely counterintuitive at first sight, but makes total sense, however, if we recall that we have adopted a determined strategy assigning $\{+\}$ to the outcome every time no clicks were measured in Alice and Bob's stations. By doing so, if it is completely impossible to receive any photon at the measurement devices ($\eta_l = 0$), we are in fact assigning $\{+\}$ to all measurements, which will lead to having all correlations equal to 1 and, thus, $S = 2$. The region that is relevant for us given that it will provide with the necessary distinguishability and efficiency to violate Bell's inequality, is the one localized in the right top of the contour plot. A more detailed plot of this area has been included in Figure 5.4. The red and blue circles designate the contour line that establishes the threshold CHSH inequality violation, as $S \geq 2$. In fact, the blue circle corresponds with the threshold we had already found in Chapter 3, $\alpha = \beta = 0.889$, as we had not included losses back then (equivalent to $\eta_l = 1$ in Figure 5.4). On the other hand, the red circle points out the minimum local efficiency required for perfect indistinguishablity, $\eta_l = 0.828$. This value agrees precisely with the fundamental limit in local efficiency required for the violation of the CHSH inequality with the maximally entangled state of two qubits [16]. In a similar way to Figure 4.2, for completeness we show the value of S as a function of the local efficiency in the limit in which photons are indistinguishable (Figure 5.5). In fact, $S = 2$ when there is no local transmission of photons due to the strategy assigning measurement outcomes, as explained above, and the violation of the inequality matches the fundamental threshold of $\eta_l = 0.828$. This is a very interesting result. When the strategy detailed in equation 5.32 was chosen, it was meant to be the simplest one: just assigning one of the two possible outcomes to every event when a click is not registered at the

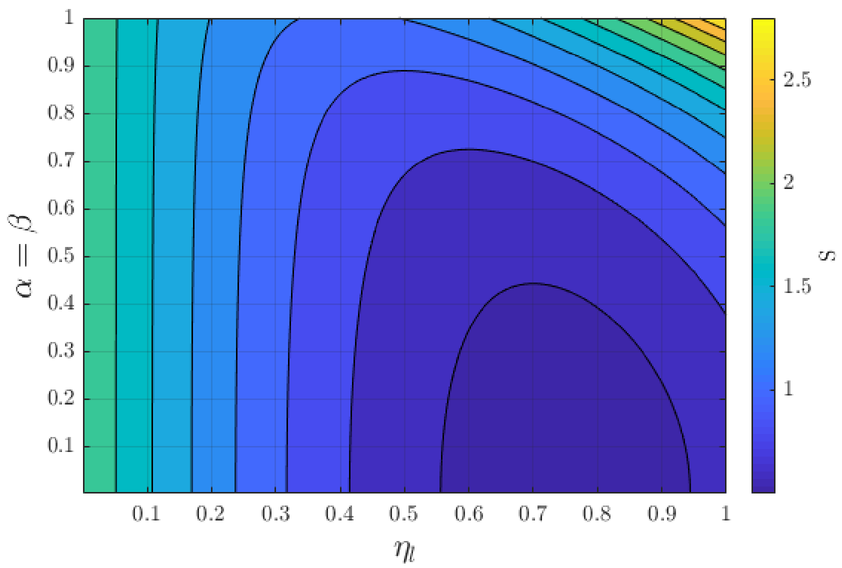

Figure 5.3: Contour map of S from the CHSH inequality in terms of the distinguishability of photons in the limit $\alpha = \beta$ and the local efficiency $\eta_l = \eta_1\eta_2(1 - T)$. The parameters have been chosen in the limit of low transmission $T \approx 0$, $\eta_t \approx 0$. The regions in which $S \geq 2$ is satisfied, are placed at both high indistinguishability and local efficiency regimes, and for a low local efficiency.

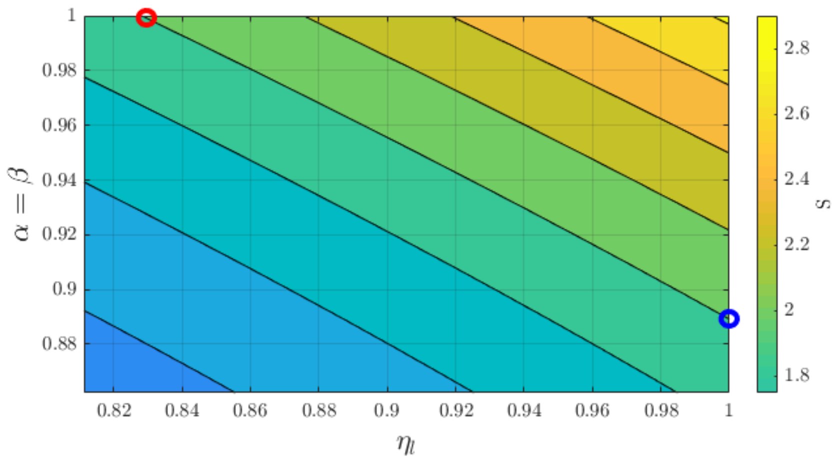

Figure 5.4: Detail from Figure 5.3, where the threshold for the violation of the CHSH inequality is clearly shown. The red and blue circles point out the contour line that delimites the regions from which $S \geq 2$. Note that the point marked by the red circle corresponds with the fundamental threshold of $\eta_l = 0.828$ [?] when photons are indistinguishable. Furthermore, when the local efficiency is perfect ($\eta_l = 1$), we recover our results from Chapter 3 and in fact, the blue circle designates a threshold in distinguishability of $\alpha = \beta = 0.889$.

detector. Furthermore, we assumed that the following step would be to find a smarter strategy. However, we have found out that the obtained threshold in local efficiency already reaches the fundamental limit for the CHSH inequality. As a consequence, we know that we can not lower the threshold by means of a better assignment of measurements. Instead, we will need to look at the dimensionality of our system or look for more suitable inequalities [18].

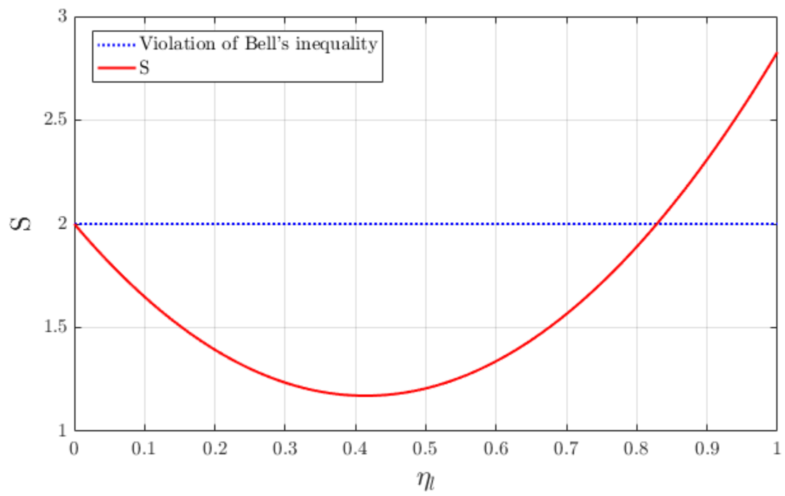

Figure 5.5: The combinations of correlations S from the CHSH inequality is plotted as a function of the local efficiency η_l, given perfect indistinguishability of photons ($\alpha = \beta = 1$).

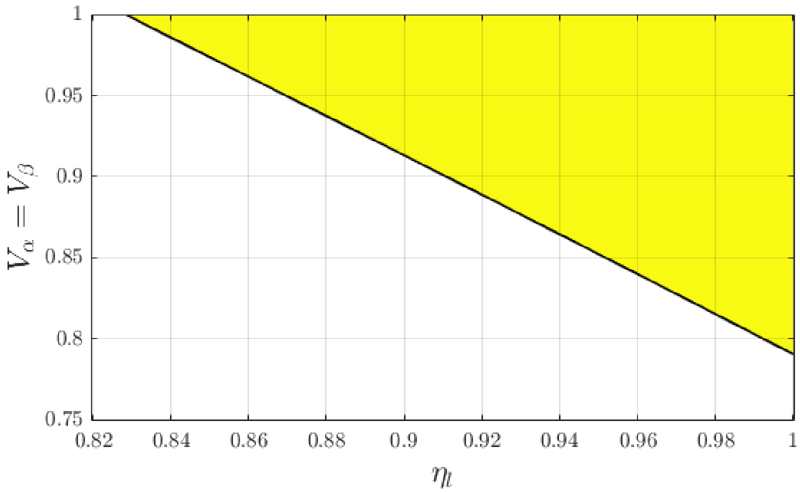

Figure 5.6: Contour map of S from the CHSH inequality in terms of the HOM visibility in the limit $\alpha = \beta$ and the local efficiency η_l. The yellow region indicates $S \geq 2$.

Whether these thresholds are actually achievable for InGaAs quantum dots as single-photon sources or not is the next big aspect of the set-up that needs to be investigated. To begin with, we translate the distinguishability of photons into the HOM visibility of the sources with equation 3.18, as we did in Chapter 3, so we can plot a contour around the threshold in visibility and local efficiency (Figure 5.6). In fact, as a sanity check, the fundamental threshold in local efficiency is indeed the same, and the required visibility of the sources in the limit of no local losses is $V_\alpha = V_\beta = 0.79$, as obtained in Chapter 3. Unfortunately, we can see that the required local efficiency is approximately $\eta_l \approx 90\%$ for reasonable efficiencies, which is not yet achievable with current InGaAs quantum-dot single-photon sources [4].

5.3.2 Optimizing the probability of transmission T

We have explored the limitations that the visibility of sources and the efficiency of transmission of the stations impose over the violation of Bell's inequality. We have approached this task in a low transmission limit T, as we showed in Figure 5.1 to ensure that the probability of correct events is dominant over the other pseudo-correct ones. But how low does it have to be, precisely? In this section we aim to find the optimal transmission T in order to answer this question and calculate quantitatively the number of times that the experiment should be run in order to violate the inequality with a certain number of σ deviations. Let us start by calculating the standard deviation σ_S of S (equation 5.40):

$$\begin{aligned}\sigma_S^2 = \langle S^2 \rangle - \langle S \rangle^2 = &\left\langle (\langle \mathbf{ab} \rangle + \langle \mathbf{a'b} \rangle + \langle \mathbf{ab'} \rangle - \langle \mathbf{a'b'} \rangle)^2 \right\rangle \\ &- \langle \langle \mathbf{ab} \rangle + \langle \mathbf{a'b} \rangle + \langle \mathbf{ab'} \rangle - \langle \mathbf{a'b'} \rangle \rangle^2\end{aligned} . \tag{5.41}$$

Expanding equation 5.41

$$\begin{aligned}\sigma_S^2 = &\left\langle \mathbf{a}^2\mathbf{b}^2 \right\rangle + \left\langle \mathbf{a}'^2\mathbf{b}^2 \right\rangle + \left\langle \mathbf{a}^2\mathbf{b}'^2 \right\rangle + \left\langle \mathbf{a}'^2\mathbf{b}'^2 \right\rangle \\ &+ 2\left\langle \langle \mathbf{ab}\rangle \langle \mathbf{a}'\mathbf{b}\rangle \right\rangle + 2\left\langle \langle \mathbf{ab}\rangle \langle \mathbf{ab}'\rangle \right\rangle + 2\left\langle \langle \mathbf{a}'\mathbf{b}\rangle \langle \mathbf{ab}'\rangle \right\rangle \\ &- 2\left\langle \langle \mathbf{ab}\rangle \langle \mathbf{a}'\mathbf{b}'\rangle \right\rangle - 2\left\langle \langle \mathbf{a}'\mathbf{b}\rangle \langle \mathbf{a}'\mathbf{b}'\rangle \right\rangle - 2\left\langle \langle \mathbf{ab}'\rangle \langle \mathbf{a}'\mathbf{b}'\rangle \right\rangle \\ &- [\langle \mathbf{ab}\rangle^2 + \langle \mathbf{a}'\mathbf{b}\rangle^2 + \langle \mathbf{ab}'\rangle^2 + \langle \mathbf{a}'\mathbf{b}'\rangle^2 \\ &+ 2\langle \mathbf{ab}\rangle \langle \mathbf{a}'\mathbf{b}\rangle + 2\langle \mathbf{ab}\rangle \langle \mathbf{ab}'\rangle + 2\langle \mathbf{a}'\mathbf{b}\rangle \langle \mathbf{ab}'\rangle \\ &- 2\langle \mathbf{ab}\rangle \langle \mathbf{a}'\mathbf{b}'\rangle - 2\langle \mathbf{a}'\mathbf{b}\rangle \langle \mathbf{a}'\mathbf{b}'\rangle - 2\langle \mathbf{ab}'\rangle \langle \mathbf{a}'\mathbf{b}'\rangle]\,.\end{aligned} \tag{5.42}$$

Note that as the four correlations $C(\mathbf{a},\mathbf{b})$ are not correlated within them, it holds for any combination of the four of them that $\langle C(\mathbf{a},\mathbf{b})C(\mathbf{a}',\mathbf{b})\rangle = \langle C(\mathbf{a},\mathbf{b})\rangle \langle C(\mathbf{a}',\mathbf{b})\rangle$, which simplifies considerably equation 5.42:

$$\begin{aligned}\sigma_S^2 &= \left\langle C^2(\mathbf{a},\mathbf{b})\right\rangle + \left\langle C^2(\mathbf{a}',\mathbf{b})\right\rangle + \left\langle C^2(\mathbf{a},\mathbf{b}')\right\rangle + \left\langle C^2(\mathbf{a}',\mathbf{b}')\right\rangle \\ &- \left[\langle C(\mathbf{a},\mathbf{b})\rangle^2 + \langle C(\mathbf{a}',\mathbf{b})\rangle^2 + \langle C(\mathbf{a},\mathbf{b}')\rangle^2 + \langle C(\mathbf{a}',\mathbf{b}')\rangle^2\right] \\ &= \sigma^2_{C(\mathbf{a},\mathbf{b})} + \sigma^2_{C(\mathbf{a}',\mathbf{b})} + \sigma^2_{C(\mathbf{a},\mathbf{b}')} + \sigma^2_{C(\mathbf{a}',\mathbf{b}')}\,.\end{aligned} \tag{5.43}$$

On the other hand, note that $\left\langle C^2(\mathbf{a},\mathbf{b})\right\rangle = \left\langle \mathbf{a}^2\mathbf{b}^2\right\rangle = 1$, attending to equation 5.40. Furthermore, it also follows that the expectation value of the expectation value gives trivially $\langle C(\mathbf{a},\mathbf{b})\rangle^2 = \langle\langle \mathbf{ab}\rangle\rangle^2 = \langle \mathbf{ab}\rangle^2 = C(\mathbf{a},\mathbf{b})^2$. Therefore we obtain a very simple expression for the standard deviation of S:

$$\sigma_S = \sqrt{4 - C(\mathbf{a},\mathbf{b})^2 - C(\mathbf{a}',\mathbf{b})^2 - C(\mathbf{a},\mathbf{b}')^2 - C(\mathbf{a}',\mathbf{b}')^2}\,. \tag{5.44}$$

However, this corresponds to the standard deviation of just one run of the experiment. The average standard deviation of S, $\bar{\sigma}_S$, has to take into account the typical number of times N_{CHS} that the photons must be sent to the heralding station in order to obtain a positive message back:

$$\bar{\sigma}_S = \frac{\sigma_S}{\sqrt{N_{CHS}}}\,. \tag{5.45}$$

Moreover, the number of heralding tries N_{CHS} is related to the actual number of runs of the experiment N_{runs} (number of attempts) by the probability of acceptance at the heralding station, P_{tot}, in the form $N_{CHS} = P_{tot}N_{runs}$. The probability of acceptance is the sum of all the probability contributions to the detection of a correct combination at the heralding station, and thus is equal to the total number of counts that we defined in equation 5.38:

$$P_{tot} = P_{2110} + P_{2011} + P_{3010} + P_{2020} + P_{2101} + P_{3100} + P_{2200} + P_{2002} + P_{3001} + P_{4000}\,. \tag{5.46}$$

Note that if the probability of acceptance was perfect, then both number of attempts would be identical. However, as this probability is lower than 1, it takes a bigger number of runs of the experiment in order to have the number of heralding events with which we calculate the averaged deviation $\bar{\sigma}_S$. We are interested, as mentioned above, in what is the best transmission T that should be used, as a low transmission improves the performance of the protocol but implies a low heralding rate and thus requires a big number of runs of the experiment. To find the best compromise we calculate the number Z of standard deviations required to violate the inequality:

$$Z = \frac{S-2}{\bar{\sigma}_S}\,, \tag{5.47}$$

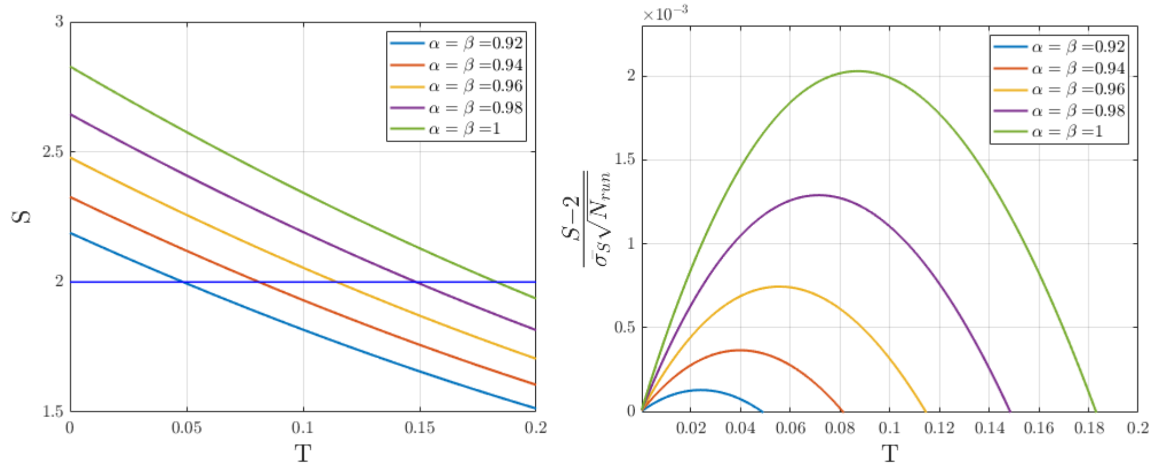

Figure 5.7: *Left.* The parameter S from the CHSH inequality is plotted for several symmetrical values of distinguishability of photons as a function of the probability of transmission of the first beam splitter. The efficiencies η_1 and η_2 have been set to 1 so it is only T that varies the global local efficiency $\eta_l = \eta_1\eta_2(1-T)$. *Right.* The number of standard deviations with respect to the violation of the inequality is plot as a function of the probability of transmission of the first beam splitter, normalized with respect to the number of times that the experiment is carried out, N_{run}. In both plots the transmission efficiency has been set to be in the low transmission limit $\eta_t = 0.1$.

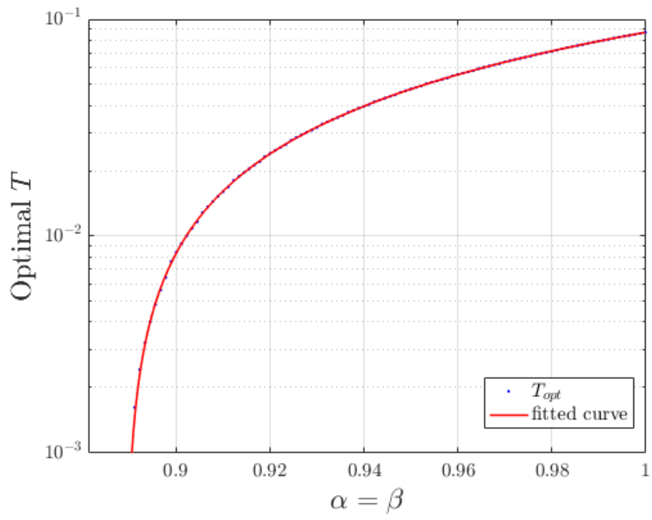

Figure 5.8: Optimal value of probability of transmission of the first beam splitter T as a function of the distinguishability of photons, in the limit of low transmission $\eta_t = 0.1$ and assuming symmetry between the sources such as $\alpha = \beta$. The optimized values have been fitted by a polynomial curve.

which applying the relations described above yields:

$$Z = \frac{S-2}{\sigma_S}\sqrt{N_{CHS}} = \frac{S-2}{\sigma_S}\sqrt{P_{tot}N_{run}}\,. \tag{5.48}$$

Thus, we can improve the number of standard deviations that we are violating Bell with by increasing the number of times we run the experiment. Z depends on the values of visibility of the sources, and has an optimal T_{opt} for each value of visibility. However, in order to proceed with the optimization over T we eliminate the dependence in number of attempts of the experiment by defining

$$Z' \equiv \frac{Z}{\sqrt{N_{run}}} = \frac{S-2}{\bar{\sigma}_S\sqrt{N_{run}}} = \frac{S-2}{\sigma_S}\sqrt{P_{tot}}\,. \tag{5.49}$$

If we stay in the realistic low transmission efficiency limit ($\eta_t \approx 0$), then we recall that P_{tot} will have only main contributions from two photons arriving to the heralding station, and thus $P_{tot} \sim T^2$. This agrees with the plots showed in Figure 5.7 Right. We can see how, in fact, for each value of distinguishability of photons there is a different optimal T with which we can achieve the maximal standard deviations from the violation of Bell's inequality. This value, and the maximum of achievable standard deviations decrease with the distinguishability of photons. This makes sense if we recall that, as the visibility of the sources decreases, being able to violate Bell's inequality gets increasingly more demanding and thus it becomes more and more important to have a very good local efficiency (as discussed in the previous section), which depends on T as $\eta_l \propto 1 - T$. To make it even simpler to visualize, the corresponding S to the displayed values of distinguishablity has been plotted on Figure 5.7 Left as a function of T. Let us now find the optimal probability of transmission for each value of distinguishability of photons. The optimization has been run for each value of distinguishability within the threshold found in the previous chapter $\alpha = \beta = 0.889$ and unity. The optimal values we find have been fitted by a polynomial fit in Figure 5.8. As expected, the optimal compromise between the heralding rate and the success of the protocol shows that the probability of transmission T should be smaller for lower values of the parameters α and β.

Finally, it would be interesting experimentally to, actually, show how many runs of experiment should be made in order to achieve a certain number of Z standard variations σ_S from the violation of the inequality. Clearing equation 5.48:

$$N_{run} = \frac{\sigma_S^2}{P_{tot}(S-2)^2}Z^2\,. \tag{5.50}$$

The number of times that the experiment should be carried out as a function of the number of standard deviations is plotted on Figure 5.9. We have taken the optimal T previously calculated for several values of the distinguishability of photons and calculate the probability of acceptance and the standard deviations corresponding to those values and each distinguishability in the low transmission limit $\eta_l \approx 0$. Notice the difference of several order of magnitude in the number of runs when comparing between close values of distinguishability.

Finally, we would like to remark that, beyond the analysis that has been done in this chapter, the correlations that we have constructed allow to calculate the viability of the experiment with precision, accounting for different inputs for visibility and efficiencies in each part of the set-up individually. We believe our work can be a useful tool for the characterization of the future experimental implementation of the protocol.

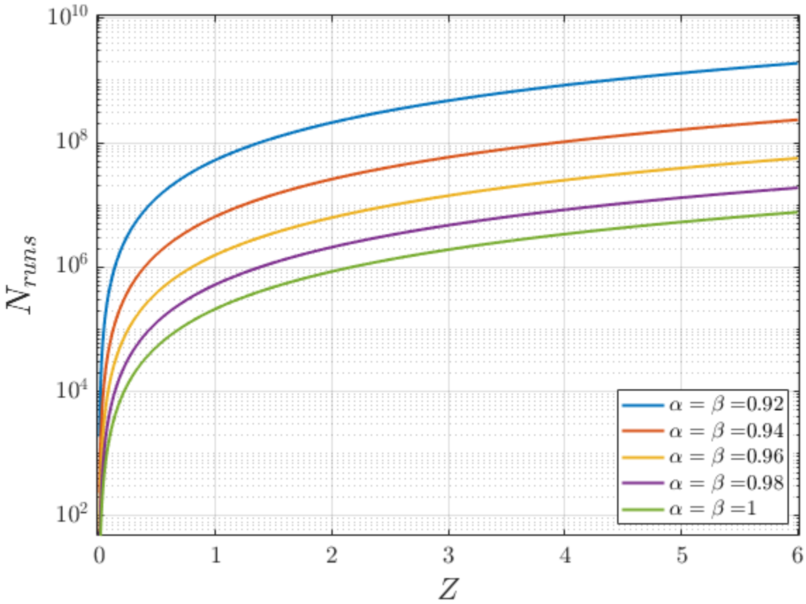

Figure 5.9: Number of times that the experiment must be run in order to achieve a Z number of standard deviations over the violation of Bell's inequality. For each value of distinguishability $\alpha = \beta$ the optimal value of probability of transmission of the first beam splitter T has been calculated in the low transmission limit $\eta_t = 0.1$.

Chapter 6

Conclusions and outlook

6.1 Conclusions

This work has allowed us to understand the experimental challenges that a Device-Independent Quantum Key Distribution protocol gives rise to. Due to the fact that its success is based on the violation of Bell's inequality, both locality and detection loopholes must be closed for its completion. While the locality loophole can be overcome by separating Alice and Bob's stations a sufficient distance, the detection loophole demands very high transmission efficiencies. To close it, we have introduced a heralding scheme [2] that has two main purposes: first, communicate to Alice and Bob whether the transmission succeeded and thus cancel the effect of the transmission inefficiencies, and create entanglement by the measurement between the pair of photons that stayed in the local stations. Furthermore, the heralding station allows knowing what is exactly the entangled state by means of the detection pattern. We can generate entanglement with 50% probability [42]; however, we stick to half of the successful events as these are the combinations of clicks that lead to a state that can be tuned in entanglement with the transmittance t of the central beam splitter of the set-up (equation 2.27).

We next have introduced several different errors in the experiment. To account for the distinguishability of photons, we related the HOM visibility of the single-photon sources to the violation of Bell's inequality. We found a threshold of approximately 79%, that is certainly achievable by single-photon sources based on InGaAs quantum dots [3]. On the other hand, we also considered mechanisms of losses in the set-up beyond the transmission between stations. This opened again the detection loophole, as the heralding does not account for local inefficiencies. In addition, the photo-detectors were not considered to be able to resolve the number of incoming photons, leading to false detection patterns in the heralding station. This two error contributions forced us to assign a determined outcome to those events in which no photons are detected by Alice and Bob, given that the fair-sampling assumption can not be done. The correlations for the CHSH inequality were constructed based on this strategy, that turned out to provide with the lowest threshold in local efficiency for indistinguishable photons achievable with the CHSH inequality, $\eta_l = 82.84\%$ [16]. In fact, we obtained a relation between the required visibility of the sources and local efficiency (Figure 5.6). Unlike the optimistic result we had found when considering only the distinguishability of photons, the required local efficiencies for typical InGaAs quantum-dot single-photon sources ($\eta_l \approx 90\%$) are not yet achievable with state-of-the-art photonic implementations [4].

Finally, we explored how to find the optimal probability of transmission T of the local beam splitters. While a high transmittance increases the heralding rate, it also enhances the probability of false messages of success from the heralding station. To find the best compromise between both situations, we calculated the number of standard deviations from the violation of the inequality as a function of T (Figure 5.7). The optimal probability of transmission decreases as photons become more distinguishable. We performed this optimization for all the possible values of distinguishability, thus being able to represent the number of expected times that the experiment should be run in order to achieve a certain number of standard deviations (Figure 5.9). Given that the repetition rate of the laser used to excite the InGaAs quantum dots is typically 72MHz, our results showed that achieving several standard deviations over the violation of Bell's inequality can be accomplished in a reasonable experimental time. However, we must remark that for this last optimization the only source of local inefficiency that was considered is T, thus assuming no losses in local transmission, which is far from reality as explained.

6.2 Outlook

The next step to take regarding further errors in the experiment should be to introduce the possibility of multiphoton generation by the single-photon sources. We can study its effect on the success of the protocol by analyzing the connection between the second-order correlation function $g^{(2)}$ and the violation of Bell's inequality. Furthermore, we have not studied yet the visibilities of the single-photon sources in relation to the actual decoherence mechanisms of InGaAs quantum dots. In the thesis, we have worked with the distinguishability parameters α and β averaged over several mode shapes; however, a noise model is required in order to calculate them precisely as this time average is not trivial.

Moreover, we have focused on how to close the detection loophole by means of high enough efficiencies using the CHSH inequality with a maximally entangled state. As explained, there is yet another approach, which consists on using an inequality that already accounts for non-detection events instead, like Eberhard's inequality [18]. This inequality finds its maximal violation with non-maximally entangled states, that can be generated with the already chosen detection pattern at the CHS and tuned with the transmittance t of the central beam splitter. This way we expect to lower the efficiency threshold down to approximately 66% although we can not predict the effect of the distinguishability of photons on this result.

Appendix A

Probability contributions

All the detailed results for the different probability contributions depicted in Chapter 4 (see Table 5.1) are detailed in this appendix. The calculation of the corresponding expectation values of the creation operators of photons at the heralded station and of lost photons can be found in Chapters 4 and 2, respectively. For each contribution the transformation of the initial operators is specified as well as the final result for the corresponding probability for each projection on the detectors.

Contribution P_{2020}

$$\begin{cases} \hat{a}^\dagger_{H_{f1}} & \to \sqrt{\frac{\eta_{1_{f1}}\eta_t T}{2}}\hat{O}^\dagger_{f1} \\ \hat{a}^\dagger_{V_{f2}} & \to \sqrt{\frac{\eta_{1_{f2}}\eta_t T}{2}}\hat{O}^\dagger_{f2} \\ \hat{b}^\dagger_{H_{f3}} & \to i\sqrt{\eta_{1_{f3}}\eta_{2_{f3}}(1-T)}b^\dagger_{H_{f3}} \\ \hat{b}^\dagger_{V_{f4}} & \to i\sqrt{\eta_{1_{f4}}\eta_{2_{f4}}(1-T)}b^\dagger_{V_{f4}} \end{cases} \tag{A.1}$$

giving:

$$\begin{aligned} \hat{a}^\dagger_{H_{f1}}\hat{a}^\dagger_{V_{f2}} &\to \frac{\eta_t T}{2}\sqrt{\eta_{1_{f1}}\eta_{1_{f2}}}\hat{O}^\dagger_{f1}\hat{O}^\dagger_{f2} \\ \hat{b}^\dagger_{H_{f3}}\hat{b}^\dagger_{V_{f4}} &\to -(1-T)\sqrt{\eta_{1_{f3}}\eta_{1_{f4}}\eta_{2_{f3}}\eta_{2_{f4}}}b^\dagger_{H_{f3}}b^\dagger_{V_{f4}} \end{aligned} \tag{A.2}$$

$$\begin{aligned} P_{2020_{SD+}} &= P_{2020_{SD-}} \\ &= \frac{\eta_t^2 T^2(1-T)^2}{4}\eta_{1_{f1}}\eta_{1_{f2}}\eta_{1_{f3}}\eta_{1_{f4}}\eta_{2_{f3}}\eta_{2_{f4}}\left\langle \hat{O}_{f1}\hat{O}_{f2}\hat{O}^\dagger_{f1}\hat{O}^\dagger_{f2}\right\rangle (1+\alpha_{34}^2)\Lambda_B K_B \\ P_{2020_{DD}} &= \\ &= \frac{\eta_t^2 T^2(1-T)^2}{4}\eta_{1_{f1}}\eta_{1_{f2}}\eta_{1_{f3}}\eta_{1_{f4}}\eta_{2_{f3}}\eta_{2_{f4}}\left\langle \hat{O}_{f1}\hat{O}_{f2}\hat{O}^\dagger_{f1}\hat{O}^\dagger_{f2}\right\rangle (\Lambda_B^2+K_B^2-2\Lambda_B K_B\alpha_{34}^2) \end{aligned} \tag{A.3}$$

Contributions to P_{2101}

$\mathbf{P_{2101_{AB}}}$

$$\begin{cases} \hat{a}^\dagger_{H_{f1}} & \to \sqrt{\frac{\eta_{1_{f1}}\eta_t T}{2}}\hat{O}^\dagger_{f1} + i\sqrt{\eta_{1_{f1}}\eta_{2_{f1}}(1-T)}\hat{a}^\dagger_{H_{f1}} \\ \hat{a}^\dagger_{V_{f2}} & \to \sqrt{\frac{\eta_{1_{f2}}\eta_t T}{2}}\hat{O}^\dagger_{f2} + i\sqrt{\eta_{1_{f2}}\eta_{2_{f2}}(1-T)}\hat{a}^\dagger_{V_{f2}} \\ \hat{b}^\dagger_{H_{f3}} & \to \sqrt{\frac{\eta_{1_{f3}}\eta_t T}{2}}\hat{O}^\dagger_{f3} + \hat{L}^\dagger_{f3} \\ \hat{b}^\dagger_{V_{f4}} & \to \sqrt{\frac{\eta_{1_{f4}}\eta_t T}{2}}\hat{O}^\dagger_{f4} + \hat{L}^\dagger_{f4} \end{cases} \tag{A.4}$$

restricted to:

$$\begin{aligned} \hat{a}^\dagger_{H_{f1}}\hat{a}^\dagger_{V_{f2}} &\to i\sqrt{\frac{\eta_{1_{f1}}\eta_{1_{f2}}\eta_t T(1-T)}{2}}\left(\sqrt{\eta_{2_{f2}}}\hat{O}^\dagger_{f1}\hat{a}^\dagger_{V_{f2}} + \sqrt{\eta_{2_{f1}}}\hat{O}^\dagger_{f2}\hat{a}^\dagger_{H_{f1}}\right) \\ \hat{b}^\dagger_{H_{f3}}\hat{b}^\dagger_{V_{f4}} &\to \sqrt{\frac{\eta_t T}{2}}\left(\sqrt{\eta_{1_{f3}}}\hat{O}^\dagger_{f3}\hat{L}^\dagger_{f4} + \sqrt{\eta_{1_{f4}}}\hat{O}^\dagger_{f4}\hat{L}^\dagger_{f3}\right) \end{aligned} \tag{A.5}$$

$$\begin{aligned} P_{2101_{AB_+}} =& \frac{\eta_t^2 T^2(1-T)}{4}\eta_{1_{f1}}\eta_{1_{f2}}\cdot \\ & [\Lambda_A\eta_{2_{f1}}\left(\eta_{1_{f3}}\left\langle \hat{O}_{f2}\hat{O}_{f3}\hat{O}^\dagger_{f2}\hat{O}^\dagger_{f3}\right\rangle\left\langle \hat{L}_{f4}\hat{L}^\dagger_{f4}\right\rangle + \eta_{1_{f4}}\left\langle \hat{O}_{f2}\hat{O}_{f4}\hat{O}^\dagger_{f2}\hat{O}^\dagger_{f4}\right\rangle\left\langle \hat{L}_{f3}\hat{L}^\dagger_{f3}\right\rangle\right) \\ & +K_A\eta_{2_{f2}}\left(\eta_{1_{f3}}\left\langle \hat{O}_{f1}\hat{O}_{f3}\hat{O}^\dagger_{f1}\hat{O}^\dagger_{f3}\right\rangle\left\langle \hat{L}_{f4}\hat{L}^\dagger_{f4}\right\rangle + \eta_{1_{f4}}\left\langle \hat{O}_{f1}\hat{O}_{f4}\hat{O}^\dagger_{f1}\hat{O}^\dagger_{f4}\right\rangle\left\langle \hat{L}_{f3}\hat{L}^\dagger_{f3}\right\rangle\right)] \\ P_{2101_{AB_-}} =& \frac{\eta_t^2 T^2(1-T)}{4}\eta_{1_{f1}}\eta_{1_{f2}}\cdot \\ & [K_A\eta_{2_{f1}}\left(\eta_{1_{f3}}\left\langle \hat{O}_{f2}\hat{O}_{f3}\hat{O}^\dagger_{f2}\hat{O}^\dagger_{f3}\right\rangle\left\langle \hat{L}_{f4}\hat{L}^\dagger_{f4}\right\rangle + \eta_{1_{f4}}\left\langle \hat{O}_{f2}\hat{O}_{f4}\hat{O}^\dagger_{f2}\hat{O}^\dagger_{f4}\right\rangle\left\langle \hat{L}_{f3}\hat{L}^\dagger_{f3}\right\rangle\right) \\ & +\Lambda_A\eta_{2_{f2}}\left(\eta_{1_{f3}}\left\langle \hat{O}_{f1}\hat{O}_{f3}\hat{O}^\dagger_{f1}\hat{O}^\dagger_{f3}\right\rangle\left\langle \hat{L}_{f4}\hat{L}^\dagger_{f4}\right\rangle + \eta_{1_{f4}}\left\langle \hat{O}_{f1}\hat{O}_{f4}\hat{O}^\dagger_{f1}\hat{O}^\dagger_{f4}\right\rangle\left\langle \hat{L}_{f3}\hat{L}^\dagger_{f3}\right\rangle\right)] \end{aligned} \tag{A.6}$$

$\mathbf{P_{2101_{BB}}}$

$$\begin{cases} \hat{a}^\dagger_{H_{f1}} & \to i\sqrt{\eta_{1_{f1}}\eta_{2_{f1}}(1-T)}\hat{a}^\dagger_{H_{f1}} + \hat{L}^\dagger_{f1} \\ \hat{a}^\dagger_{V_{f2}} & \to i\sqrt{\eta_{1_{f2}}\eta_{2_{f2}}(1-T)}\hat{a}^\dagger_{V_{f2}} + \hat{L}^\dagger_{f2} \\ \hat{b}^\dagger_{H_{f3}} & \to \sqrt{\frac{\eta_{1_{f3}}\eta_t T}{2}}\hat{O}^\dagger_{f3} \\ \hat{b}^\dagger_{V_{f4}} & \to \sqrt{\frac{\eta_{1_{f4}}\eta_t T}{2}}\hat{O}^\dagger_{f4} \end{cases} \tag{A.7}$$

restricted to:

$$\begin{aligned} \hat{a}^\dagger_{H_{f1}}\hat{a}^\dagger_{V_{f2}} &\to -\sqrt{1-T}\left(\sqrt{\eta_{1_{f1}}\eta_{2_{f1}}}\hat{a}^\dagger_{H_{f1}}\hat{L}^\dagger_{f2} + \sqrt{\eta_{1_{f2}}\eta_{2_{f2}}}\hat{a}^\dagger_{V_{f2}}\hat{L}^\dagger_{f1}\right) \\ \hat{b}^\dagger_{H_{f3}}\hat{b}^\dagger_{V_{f4}} &\to \frac{\eta_t T}{2}\sqrt{\eta_{1_{f3}}\eta_{1_{f4}}}\hat{O}^\dagger_{f3}\hat{O}^\dagger_{f4} \end{aligned} \tag{A.8}$$

$$
\begin{aligned}
P_{2101_{BB_+}} =& \frac{\eta_t^2 T^2(1-T)}{4}\eta_{1_{f3}}\eta_{1_{f4}}\left\langle \hat{O}_{f3}\hat{O}_{f4}\hat{O}^\dagger_{f3}\hat{O}^\dagger_{f4}\right\rangle\left[\Lambda_A\eta_{1_{f1}}\eta_{2_{f1}}\left\langle\hat{L}_{f2}\hat{L}^\dagger_{f2}\right\rangle + K_A\eta_{1_{f2}}\eta_{2_{f2}}\left\langle\hat{L}_{f1}\hat{L}^\dagger_{f1}\right\rangle\right]\\
P_{2101_{BB_-}} =& \frac{\eta_t^2 T^2(1-T)}{4}\eta_{1_{f3}}\eta_{1_{f4}}\left\langle \hat{O}_{f3}\hat{O}_{f4}\hat{O}^\dagger_{f3}\hat{O}^\dagger_{f4}\right\rangle\left[K_A\eta_{1_{f1}}\eta_{2_{f1}}\left\langle\hat{L}_{f2}\hat{L}^\dagger_{f2}\right\rangle + \Lambda_A\eta_{1_{f2}}\eta_{2_{f2}}\left\langle\hat{L}_{f1}\hat{L}^\dagger_{f1}\right\rangle\right]
\end{aligned}
\tag{A.9}
$$

Contributions to P_{2101}

$\mathbf{P_{2011_{AB}}}$

$$
\begin{cases}
\hat{a}^\dagger_{H_{f1}} & \rightarrow \sqrt{\frac{\eta_{1_{f1}}\eta_t T}{2}}\hat{O}^\dagger_{f1} + \hat{L}^\dagger_{f1}\\
\hat{a}^\dagger_{V_{f2}} & \rightarrow \sqrt{\frac{\eta_{1_{f2}}\eta_t T}{2}}\hat{O}^\dagger_{f2} + \hat{L}^\dagger_{f2}\\
\hat{b}^\dagger_{H_{f3}} & \rightarrow \sqrt{\frac{\eta_{1_{f3}}\eta_t T}{2}}\hat{O}^\dagger_{f3} + i\sqrt{\eta_{1_{f3}}\eta_{2_{f3}}(1-T)}b^\dagger_{H_{f3}}\\
\hat{b}^\dagger_{V_{f4}} & \rightarrow \sqrt{\frac{\eta_{1_{f4}}\eta_t T}{2}}\hat{O}^\dagger_{f4} + i\sqrt{\eta_{1_{f4}}\eta_{2_{f4}}(1-T)}b^\dagger_{V_{f4}}
\end{cases}
\tag{A.10}
$$

restricted to:

$$
\begin{aligned}
\hat{a}^\dagger_{H_{f1}}\hat{a}^\dagger_{V_{f2}} &\rightarrow \sqrt{\frac{\eta_t T}{2}}\left(\sqrt{\eta_{1_{f1}}}\hat{O}^\dagger_{f1}\hat{L}^\dagger_{f2} + \sqrt{\eta_{1_{f2}}}\hat{O}^\dagger_{f2}\hat{L}^\dagger_{f1}\right)\\
\hat{b}^\dagger_{H_{f3}}\hat{b}^\dagger_{V_{f4}} &\rightarrow i\sqrt{\frac{\eta_{1_{f3}}\eta_{1_{f4}}\eta_t T(1-T)}{2}}\left(\sqrt{\eta_{2_{f4}}}\hat{O}^\dagger_{f3}\hat{b}^\dagger_{V_{f4}} + \sqrt{\eta_{2_{f3}}}\hat{O}^\dagger_{f4}\hat{b}^\dagger_{H_{f3}}\right)
\end{aligned}
\tag{A.11}
$$

$$
\begin{aligned}
P_{2011_{AB_+}} =& \frac{\eta_t^2 T^2(1-T)}{4}\eta_{1_{f3}}\eta_{1_{f4}}\cdot\\
&[\Lambda_B\eta_{2_{f3}}\left(\eta_{1_{f1}}\left\langle\hat{O}_{f1}\hat{O}_{f4}\hat{O}^\dagger_{f1}\hat{O}^\dagger_{f4}\right\rangle\left\langle\hat{L}_{f2}\hat{L}^\dagger_{f2}\right\rangle + \eta_{1_{f2}}\left\langle\hat{O}_{f2}\hat{O}_{f4}\hat{O}^\dagger_{f2}\hat{O}^\dagger_{f4}\right\rangle\left\langle\hat{L}_{f1}\hat{L}^\dagger_{f1}\right\rangle\right)\\
&+K_B\eta_{2_{f4}}\left(\eta_{1_{f1}}\left\langle\hat{O}_{f1}\hat{O}_{f3}\hat{O}^\dagger_{f1}\hat{O}^\dagger_{f3}\right\rangle\left\langle\hat{L}_{f2}\hat{L}^\dagger_{f2}\right\rangle + \eta_{1_{f2}}\left\langle\hat{O}_{f2}\hat{O}_{f3}\hat{O}^\dagger_{f2}\hat{O}^\dagger_{f3}\right\rangle\left\langle\hat{L}_{f1}\hat{L}^\dagger_{f1}\right\rangle\right)]\\
P_{2011_{AB_-}} =& \frac{\eta_t^2 T^2(1-T)}{4}\eta_{1_{f3}}\eta_{1_{f4}}\cdot\\
&[K_B\eta_{2_{f3}}\left(\eta_{1_{f1}}\left\langle\hat{O}_{f1}\hat{O}_{f4}\hat{O}^\dagger_{f1}\hat{O}^\dagger_{f4}\right\rangle\left\langle\hat{L}_{f2}\hat{L}^\dagger_{f2}\right\rangle + \eta_{1_{f2}}\left\langle\hat{O}_{f2}\hat{O}_{f4}\hat{O}^\dagger_{f2}\hat{O}^\dagger_{f4}\right\rangle\left\langle\hat{L}_{f1}\hat{L}^\dagger_{f1}\right\rangle\right)\\
&+\Lambda_B\eta_{2_{f4}}\left(\eta_{1_{f1}}\left\langle\hat{O}_{f1}\hat{O}_{f3}\hat{O}^\dagger_{f1}\hat{O}^\dagger_{f3}\right\rangle\left\langle\hat{L}_{f2}\hat{L}^\dagger_{f2}\right\rangle + \eta_{1_{f2}}\left\langle\hat{O}_{f2}\hat{O}_{f3}\hat{O}^\dagger_{f2}\hat{O}^\dagger_{f3}\right\rangle\left\langle\hat{L}_{f1}\hat{L}^\dagger_{f1}\right\rangle\right)]
\end{aligned}
\tag{A.12}
$$

$\mathbf{P_{2011_{AA}}}$

$$
\begin{cases}
\hat{a}^\dagger_{H_{f1}} & \rightarrow \sqrt{\frac{\eta_{1_{f1}}\eta_t T}{2}}\hat{O}^\dagger_{f1}\\
\hat{a}^\dagger_{V_{f2}} & \rightarrow \sqrt{\frac{\eta_{1_{f2}}\eta_t T}{2}}\hat{O}^\dagger_{f2}\\
\hat{b}^\dagger_{H_{f3}} & \rightarrow i\sqrt{\eta_{1_{f3}}\eta_{2_{f3}}(1-T)}b^\dagger_{H_{f3}} + \hat{L}^\dagger_{f3}\\
\hat{b}^\dagger_{V_{f4}} & \rightarrow i\sqrt{\eta_{1_{f4}}\eta_{2_{f4}}(1-T)}b^\dagger_{V_{f4}} + \hat{L}^\dagger_{f4}
\end{cases}
\tag{A.13}
$$

restricted to:

$$\begin{aligned} \hat{a}^\dagger_{H_{f1}}\hat{a}^\dagger_{V_{f2}} &\to \frac{\eta_t T}{2}\sqrt{\eta_{1_{f1}}\eta_{1_{f2}}}\hat{O}^\dagger_{f1}\hat{O}^\dagger_{f2} \\ \hat{b}^\dagger_{H_{f3}}\hat{b}^\dagger_{V_{f4}} &\to -\sqrt{1-T}\left(\sqrt{\eta_{1_{f3}}\eta_{2_{f3}}}\hat{b}^\dagger_{H_{f3}}\hat{L}^\dagger_{f4} + \sqrt{\eta_{1_{f4}}\eta_{2_{f4}}}\hat{b}^\dagger_{V_{f4}}\hat{L}^\dagger_{f3}\right) \end{aligned} \tag{A.14}$$

$$\begin{aligned} P_{2011_{AA_+}} =& \frac{\eta_t^2 T^2(1-T)}{4}\eta_{1_{f1}}\eta_{1_{f2}}\left\langle \hat{O}_{f1}\hat{O}_{f2}\hat{O}^\dagger_{f1}\hat{O}^\dagger_{f2}\right\rangle\left[\Lambda_B\eta_{1_{f3}}\eta_{2_{f3}}\left\langle\hat{L}_{f4}\hat{L}^\dagger_{f4}\right\rangle + K_B\eta_{1_{f4}}\eta_{2_{f4}}\left\langle\hat{L}_{f3}\hat{L}^\dagger_{f3}\right\rangle\right] \\ P_{2011_{AA_-}} =& \frac{\eta_t^2 T^2(1-T)}{4}\eta_{1_{f1}}\eta_{1_{f2}}\left\langle \hat{O}_{f1}\hat{O}_{f2}\hat{O}^\dagger_{f1}\hat{O}^\dagger_{f2}\right\rangle\left[K_B\eta_{1_{f3}}\eta_{2_{f3}}\left\langle\hat{L}_{f4}\hat{L}^\dagger_{f4}\right\rangle + \Lambda_B\eta_{1_{f4}}\eta_{2_{f4}}\left\langle\hat{L}_{f3}\hat{L}^\dagger_{f3}\right\rangle\right] \end{aligned} \tag{A.15}$$

Contributions to P_{2002}

$\mathbf{P_{2002_{AB}}}$

$$\begin{cases} \hat{a}^\dagger_{H_{f1}} & \to \sqrt{\frac{\eta_{1_{f1}}\eta_t T}{2}}\hat{O}^\dagger_{f1} + \hat{L}^\dagger_{f1} \\ \hat{a}^\dagger_{V_{f2}} & \to \sqrt{\frac{\eta_{1_{f2}}\eta_t T}{2}}\hat{O}^\dagger_{f2} + \hat{L}^\dagger_{f2} \\ \hat{b}^\dagger_{H_{f3}} & \to \sqrt{\frac{\eta_{1_{f3}}\eta_t T}{2}}\hat{O}^\dagger_{f3} + \hat{L}^\dagger_{f3} \\ \hat{b}^\dagger_{V_{f4}} & \to \sqrt{\frac{\eta_{1_{f4}}\eta_t T}{2}}\hat{O}^\dagger_{f4} + \hat{L}^\dagger_{f4} \end{cases} \tag{A.16}$$

restricted to:

$$\begin{aligned} \hat{a}^\dagger_{H_{f1}}\hat{a}^\dagger_{V_{f2}} &\to \sqrt{\frac{\eta_t T}{2}}\left(\sqrt{\eta_{1_{f1}}}\hat{O}^\dagger_{f1}\hat{L}^\dagger_{f2} + \sqrt{\eta_{1_{f2}}}\hat{O}^\dagger_{f2}\hat{L}^\dagger_{f1}\right) \\ \hat{b}^\dagger_{H_{f3}}\hat{b}^\dagger_{V_{f4}} &\to \sqrt{\frac{\eta_t T}{2}}\left(\sqrt{\eta_{1_{f3}}}\hat{O}^\dagger_{f3}\hat{L}^\dagger_{f4} + \sqrt{\eta_{1_{f4}}}\hat{O}^\dagger_{f4}\hat{L}^\dagger_{f3}\right) \end{aligned} \tag{A.17}$$

$$\begin{aligned} P_{2002_{AB}} =& \frac{\eta_t^2 T^2}{4}\cdot \\ & [\eta_{1_{f1}}\eta_{1_{f3}}\left\langle\hat{O}_{f1}\hat{O}_{f3}\hat{O}^\dagger_{f1}\hat{O}^\dagger_{f3}\right\rangle\left\langle\hat{L}_{f2}\hat{L}_{f4}\hat{L}^\dagger_{f2}\hat{L}^\dagger_{f4}\right\rangle + \eta_{1_{f1}}\eta_{1_{f4}}\left\langle\hat{O}_{f1}\hat{O}_{f4}\hat{O}^\dagger_{f1}\hat{O}^\dagger_{f4}\right\rangle\left\langle\hat{L}_{f2}\hat{L}_{f3}\hat{L}^\dagger_{f2}\hat{L}^\dagger_{f3}\right\rangle \\ & +\eta_{1_{f2}}\eta_{1_{f3}}\left\langle\hat{O}_{f2}\hat{O}_{f3}\hat{O}^\dagger_{f2}\hat{O}^\dagger_{f3}\right\rangle\left\langle\hat{L}_{f1}\hat{L}_{f4}\hat{L}^\dagger_{f1}\hat{L}^\dagger_{f4}\right\rangle + \eta_{1_{f2}}\eta_{1_{f4}}\left\langle\hat{O}_{f2}\hat{O}_{f4}\hat{O}^\dagger_{f2}\hat{O}^\dagger_{f4}\right\rangle\left\langle\hat{L}_{f1}\hat{L}_{f3}\hat{L}^\dagger_{f1}\hat{L}^\dagger_{f3}\right\rangle] \end{aligned} \tag{A.18}$$

$\mathbf{P_{2002_{AA}}}$

Trivially:

$$\begin{aligned} \hat{a}^\dagger_{H_{f1}}\hat{a}^\dagger_{V_{f2}} &\to \frac{\eta_t T}{2}\sqrt{\eta_{1_{f1}}\eta_{1_{f2}}}\hat{O}^\dagger_{f1}\hat{O}^\dagger_{f2} \\ \hat{b}^\dagger_{H_{f3}}\hat{b}^\dagger_{V_{f4}} &\to \hat{L}^\dagger_{f3}\hat{L}^\dagger_{f4} \end{aligned} \tag{A.19}$$

$$P_{2002_{AA}} = \frac{\eta_t^2 T^2}{4}\eta_{1_{f1}}\eta_{1_{f2}}\left\langle\hat{O}_{f1}\hat{O}_{f2}\hat{O}^\dagger_{f1}\hat{O}^\dagger_{f2}\right\rangle\left\langle\hat{L}_{f3}\hat{L}_{f4}\hat{L}^\dagger_{f3}\hat{L}^\dagger_{f4}\right\rangle \tag{A.20}$$

$$\tag{A.21}$$

$\mathbf{P_{2002_{BB}}}$

Trivially:

$$\begin{aligned}\hat{a}^\dagger_{H_{f1}}\hat{a}^\dagger_{V_{f2}} &\to \hat{L}^\dagger_{f1}\hat{L}^\dagger_{f2}\\ \hat{b}^\dagger_{H_{f3}}\hat{b}^\dagger_{V_{f4}} &\to \frac{\eta_t T}{2}\sqrt{\eta_{1_{f3}}\eta_{1_{f4}}}\hat{O}^\dagger_{f3}\hat{O}^\dagger_{f4}\end{aligned} \tag{A.22}$$

$$P_{2002_{BB}} = \frac{\eta_t^2 T^2}{4}\eta_{1_{f3}}\eta_{1_{f4}}\left\langle \hat{O}_{f3}\hat{O}_{f4}\hat{O}^\dagger_{f3}\hat{O}^\dagger_{f4}\right\rangle \left\langle \hat{L}_{f1}\hat{L}_{f2}\hat{L}^\dagger_{f1}\hat{L}^\dagger_{f2}\right\rangle \tag{A.23}$$

Contributions P_{3100} and P_{3010}

$\mathbf{P_{3100}}$

$$\begin{cases}\hat{a}^\dagger_{H_{f1}} & \to \sqrt{\frac{\eta_{1_{f1}}\eta_t T}{2}}\hat{O}^\dagger_{f1} + i\sqrt{\eta_{1_{f1}}\eta_{2_{f1}}(1-T)}\hat{a}^\dagger_{H_{f1}}\\ \hat{a}^\dagger_{V_{f2}} & \to \sqrt{\frac{\eta_{1_{f2}}\eta_t T}{2}}\hat{O}^\dagger_{f2} + i\sqrt{\eta_{1_{f2}}\eta_{2_{f2}}(1-T)}\hat{a}^\dagger_{V_{f2}}\\ b^\dagger_{H_{f3}} & \to \sqrt{\frac{\eta_{1_{f3}}\eta_t T}{2}}\hat{O}^\dagger_{f3}\\ b^\dagger_{V_{f4}} & \to \sqrt{\frac{\eta_{1_{f4}}\eta_t T}{2}}\hat{O}^\dagger_{f4}\end{cases} \tag{A.24}$$

restricted to:

$$\begin{aligned}\hat{a}^\dagger_{H_{f1}}\hat{a}^\dagger_{V_{f2}} &\to i\sqrt{\frac{\eta_{1_{f1}}\eta_{1_{f2}}\eta_t T(1-T)}{2}}\left(\sqrt{\eta_{2_{f2}}}\hat{O}^\dagger_{f1}\hat{a}^\dagger_{V_{f2}} + \sqrt{\eta_{2_{f1}}}\hat{O}^\dagger_{f2}\hat{a}^\dagger_{H_{f1}}\right)\\ \hat{b}^\dagger_{H_{f3}}\hat{b}^\dagger_{V_{f4}} &\to \frac{\eta_t T}{2}\sqrt{\eta_{1_{f3}}\eta_{1_{f4}}}\hat{O}^\dagger_{f3}\hat{O}^\dagger_{f4}\end{aligned} \tag{A.25}$$

$$\begin{aligned}P_{3100_+} =& \frac{\eta_t^3 T^3(1-T)}{8}\eta_{1_{f1}}\eta_{1_{f2}}\eta_{1_{f3}}\eta_{1_{f4}}\cdot\\ &\left(\Lambda_A\eta_{2_{f1}}\left\langle \hat{O}_{f2}\hat{O}_{f3}\hat{O}_{f4}\hat{O}^\dagger_{f2}\hat{O}^\dagger_{f3}\hat{O}^\dagger_{f4}\right\rangle + K_A\eta_{2_{f2}}\left\langle \hat{O}_{f1}\hat{O}_{f3}\hat{O}_{f4}\hat{O}^\dagger_{f1}\hat{O}^\dagger_{f3}\hat{O}^\dagger_{f4}\right\rangle\right)\\ P_{3100_-} =& \frac{\eta_t^3 T^3(1-T)}{8}\eta_{1_{f1}}\eta_{1_{f2}}\eta_{1_{f3}}\eta_{1_{f4}}\cdot\\ &\left(K_A\eta_{2_{f1}}\left\langle \hat{O}_{f2}\hat{O}_{f3}\hat{O}_{f4}\hat{O}^\dagger_{f2}\hat{O}^\dagger_{f3}\hat{O}^\dagger_{f4}\right\rangle + \Lambda_A\eta_{2_{f2}}\left\langle \hat{O}_{f1}\hat{O}_{f3}\hat{O}_{f4}\hat{O}^\dagger_{f1}\hat{O}^\dagger_{f3}\hat{O}^\dagger_{f4}\right\rangle\right)\end{aligned} \tag{A.26}$$

$\mathbf{P_{3010}}$

$$\begin{cases}\hat{a}^\dagger_{H_{f1}} & \to \sqrt{\frac{\eta_{1_{f1}}\eta_t T}{2}}\hat{O}^\dagger_{f1}\\ \hat{a}^\dagger_{V_{f2}} & \to \sqrt{\frac{\eta_{1_{f2}}\eta_t T}{2}}\hat{O}^\dagger_{f2}\\ b^\dagger_{H_{f3}} & \to \sqrt{\frac{\eta_{1_{f3}}\eta_t T}{2}}\hat{O}^\dagger_{f3} + i\sqrt{\eta_{1_{f3}}\eta_{2_{f3}}(1-T)}b^\dagger_{H_{f3}}\\ b^\dagger_{V_{f4}} & \to \sqrt{\frac{\eta_{1_{f4}}\eta_t T}{2}}\hat{O}^\dagger_{f4} + i\sqrt{\eta_{1_{f4}}\eta_{2_{f4}}(1-T)}b^\dagger_{V_{f4}}\end{cases} \tag{A.27}$$

restricted to:

$$\begin{aligned}
&\hat{a}^\dagger_{H_{f1}}\hat{a}^\dagger_{V_{f2}} \rightarrow \frac{\eta_t T}{2}\sqrt{\eta_{1_{f1}}\eta_{1_{f2}}}\hat{O}^\dagger_{f1}\hat{O}^\dagger_{f2}\\
&\hat{b}^\dagger_{H_{f3}}\hat{b}^\dagger_{V_{f4}} \rightarrow i\sqrt{\frac{\eta_{1_{f3}}\eta_{1_{f4}}\eta_t T(1-T)}{2}}\left(\sqrt{\eta_{2_{f4}}}\hat{O}^\dagger_{f3}\hat{b}^\dagger_{V_{f4}}+\sqrt{\eta_{2_{f3}}}\hat{O}^\dagger_{f4}\hat{b}^\dagger_{H_{f3}}\right)
\end{aligned} \tag{A.28}$$

$$\begin{aligned}
P_{3010_+} =& \frac{\eta_t^3 T^3(1-T)}{8}\eta_{1_{f1}}\eta_{1_{f2}}\eta_{1_{f3}}\eta_{1_{f4}}\cdot\\
&\left(\Lambda_B\eta_{2_{f3}}\left\langle\hat{O}_{f4}\hat{O}_{f1}\hat{O}_{f2}\hat{O}^\dagger_{f4}\hat{O}^\dagger_{f1}\hat{O}^\dagger_{f2}\right\rangle+K_B\eta_{2_{f4}}\left\langle\hat{O}_{f3}\hat{O}_{f1}\hat{O}_{f2}\hat{O}^\dagger_{f3}\hat{O}^\dagger_{f1}\hat{O}^\dagger_{f2}\right\rangle\right)\\
P_{3010_-} =& \frac{\eta_t^3 T^3(1-T)}{8}\eta_{1_{f1}}\eta_{1_{f2}}\eta_{1_{f3}}\eta_{1_{f4}}\cdot\\
&\left(K_B\eta_{2_{f3}}\left\langle\hat{O}_{f4}\hat{O}_{f1}\hat{O}_{f2}\hat{O}^\dagger_{f4}\hat{O}^\dagger_{f1}\hat{O}^\dagger_{f2}\right\rangle+\Lambda_B\eta_{2_{f4}}\left\langle\hat{O}_{f3}\hat{O}_{f1}\hat{O}_{f2}\hat{O}^\dagger_{f3}\hat{O}^\dagger_{f1}\hat{O}^\dagger_{f2}\right\rangle\right)
\end{aligned} \tag{A.29}$$

Contributions to P_{3001}

$\mathbf{P_{3001_{AAB}}}$

$$\begin{cases}
\hat{a}^\dagger_{H_{f1}} & \rightarrow \sqrt{\frac{\eta_{1_{f1}}\eta_t T}{2}}\hat{O}^\dagger_{f1}\\
\hat{a}^\dagger_{V_{f2}} & \rightarrow \sqrt{\frac{\eta_{1_{f2}}\eta_t T}{2}}\hat{O}^\dagger_{f2}\\
b^\dagger_{H_{f3}} & \rightarrow \sqrt{\frac{\eta_{1_{f3}}\eta_t T}{2}}\hat{O}^\dagger_{f3}+\hat{L}^\dagger_{f3}\\
b^\dagger_{V_{f4}} & \rightarrow \sqrt{\frac{\eta_{1_{f4}}\eta_t T}{2}}\hat{O}^\dagger_{f4}+\hat{L}^\dagger_{f4}
\end{cases} \tag{A.30}$$

restricted to:

$$\begin{aligned}
&\hat{a}^\dagger_{H_{f1}}\hat{a}^\dagger_{V_{f2}} \rightarrow \frac{\eta_t T}{2}\sqrt{\eta_{1_{f1}}\eta_{1_{f2}}}\hat{O}^\dagger_{f1}\hat{O}^\dagger_{f2}\\
&\hat{b}^\dagger_{H_{f3}}\hat{b}^\dagger_{V_{f4}} \rightarrow \sqrt{\frac{\eta_t T}{2}}\left(\sqrt{\eta_{1_{f3}}}\hat{O}^\dagger_{f3}\hat{L}^\dagger_{f4}+\sqrt{\eta_{1_{f4}}}\hat{O}^\dagger_{f4}\hat{L}^\dagger_{f3}\right)
\end{aligned} \tag{A.31}$$

$$\begin{aligned}
P_{3001_{AAB}} =& \frac{\eta_t^3 T^3}{8}\eta_{1_{f1}}\eta_{1_{f2}}\cdot\\
&\left(\eta_{1_{f3}}\left\langle\hat{O}_{f1}\hat{O}_{f2}\hat{O}_{f3}\hat{O}^\dagger_{f1}\hat{O}^\dagger_{f2}\hat{O}^\dagger_{f3}\right\rangle\left\langle\hat{L}_{f4}\hat{L}^\dagger_{f4}\right\rangle+\eta_{1_{f4}}\left\langle\hat{O}_{f1}\hat{O}_{f2}\hat{O}_{f4}\hat{O}^\dagger_{f1}\hat{O}^\dagger_{f2}\hat{O}^\dagger_{f4}\right\rangle\left\langle\hat{L}_{f3}\hat{L}^\dagger_{f3}\right\rangle\right)
\end{aligned} \tag{A.32}$$

$\mathbf{P_{3001_{ABB}}}$

$$\begin{cases}
\hat{a}^\dagger_{H_{f1}} & \rightarrow \sqrt{\frac{\eta_{1_{f1}}\eta_t T}{2}}\hat{O}^\dagger_{f1}+\hat{L}^\dagger_{f1}\\
\hat{a}^\dagger_{V_{f2}} & \rightarrow \sqrt{\frac{\eta_{1_{f2}}\eta_t T}{2}}\hat{O}^\dagger_{f2}+\hat{L}^\dagger_{f2}\\
b^\dagger_{H_{f3}} & \rightarrow \sqrt{\frac{\eta_{1_{f3}}\eta_t T}{2}}\hat{O}^\dagger_{f3}\\
b^\dagger_{V_{f4}} & \rightarrow \sqrt{\frac{\eta_{1_{f4}}\eta_t T}{2}}\hat{O}^\dagger_{f4}
\end{cases} \tag{A.33}$$

restricted to:

$$\begin{aligned}\hat{a}^\dagger_{H_{f1}}\hat{a}^\dagger_{V_{f2}} &\rightarrow \sqrt{\frac{\eta_t T}{2}}\left(\sqrt{\eta_{1_{f1}}}\hat{O}^\dagger_{f1}\hat{L}^\dagger_{f2} + \sqrt{\eta_{1_{f2}}}\hat{O}^\dagger_{f2}\hat{L}^\dagger_{f1}\right)\\ \hat{b}^\dagger_{H_{f3}}\hat{b}^\dagger_{V_{f4}} &\rightarrow \frac{\eta_t T}{2}\sqrt{\eta_{1_{f3}}\eta_{1_{f4}}}\hat{O}^\dagger_{f3}\hat{O}^\dagger_{f4}\end{aligned} \tag{A.34}$$

$$\begin{aligned}P_{3001_{ABB}} =& \frac{\eta_t^3 T^3}{8}\eta_{1_{f3}}\eta_{1_{f4}}\cdot\\ &\left(\eta_{1_{f1}}\left\langle\hat{O}_{f1}\hat{O}_{f3}\hat{O}_{f4}\hat{O}^\dagger_{f1}\hat{O}^\dagger_{f3}\hat{O}^\dagger_{f4}\right\rangle\left\langle\hat{L}_{f2}\hat{L}^\dagger_{f2}\right\rangle + \eta_{1_{f2}}\left\langle\hat{O}_{f2}\hat{O}_{f3}\hat{O}_{f4}\hat{O}^\dagger_{f2}\hat{O}^\dagger_{f3}\hat{O}^\dagger_{f4}\right\rangle\left\langle\hat{L}_{f1}\hat{L}^\dagger_{f1}\right\rangle\right)\end{aligned} \tag{A.35}$$

Contribution P_{4000}

Trivially:

$$\begin{aligned}\hat{a}^\dagger_{H_{f1}}\hat{a}^\dagger_{V_{f2}} &\rightarrow \frac{\eta_t T}{2}\sqrt{\eta_{1_{f1}}\eta_{1_{f2}}}\hat{O}^\dagger_{f1}\hat{O}^\dagger_{f2}\\ \hat{b}^\dagger_{H_{f3}}\hat{b}^\dagger_{V_{f4}} &\rightarrow \frac{\eta_t T}{2}\sqrt{\eta_{1_{f3}}\eta_{1_{f4}}}\hat{O}^\dagger_{f3}\hat{O}^\dagger_{f4}\end{aligned} \tag{A.36}$$

$$P_{4000} = \frac{\eta_t^4 T^4}{16}\eta_{1_{f1}}\eta_{1_{f2}}\eta_{1_{f3}}\eta_{1_{f4}}\left\langle\hat{O}_{f1}\hat{O}_{f2}\hat{O}_{f3}\hat{O}_{f4}\hat{O}^\dagger_{f1}\hat{O}^\dagger_{f2}\hat{O}^\dagger_{f3}\hat{O}^\dagger_{f4}\right\rangle \tag{A.37}$$

Bibliography

[1] Stefano Pironio, Antonio Acín, Nicolas Brunner, Nicolas Gisin, Serge Massar, and Valerio Scarani. Device-independent quantum key distribution secure against collective attacks. *New Journal of Physics*, 11(4):045021, apr 2009.

[2] Alejandro Máttar, Jan Kołodyński, Paul Skrzypczyk, Daniel Cavalcanti, Konrad Banaszek, and Antonio Acín. Device-independent quantum key distribution with single-photon sources. *arXiv e-prints*, page arXiv:1803.07089, Mar 2018.

[3] Gabija Kiršanskė, Henri Thyrrestrup, Raphaël S. Daveau, Chris L. Dreeßen, Tommaso Pregnolato, Leonardo Midolo, Petru Tighineanu, Alisa Javadi, Søren Stobbe, Rüdiger Schott, Arne Ludwig, Andreas D. Wieck, Suk In Park, Jin D. Song, Andreas V. Kuhlmann, Immo Söllner, Matthias C. Löbl, Richard J. Warburton, and Peter Lodahl. Indistinguishable and efficient single photons from a quantum dot in a planar nanobeam waveguide. *Phys. Rev. B*, 96:165306, Oct 2017.

[4] Thomas Hummel, Claudéric Ouellet-Plamondon, Ela Ugur, Irina Kulkova, Toke Lund-Hansen, Matthew A. Broome, Ravitej Uppu, and Peter Lodahl. Efficient demultiplexed single-photon source with a quantum dot coupled to a nanophotonic waveguide. *Applied Physics Letters*, 115(2):021102, 2019.

[5] Newport. Fiber optic basics. https://www.newport.com/t/fiber-optic-basics, 2019.

[6] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, 47:777–780, May 1935.

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

[8] D. Bohm and Y. Aharonov. Discussion of experimental proof for the paradox of einstein, rosen, and podolsky. *Phys. Rev.*, 108:1070–1076, Nov 1957.

[9] Christopher Gerry and Peter Knight. *Introductory Quantum Optics*. Cambridge University Press, 2004.

[10] Jun J. Sakurai and Henry S. Valk. Advanced quantum mechanics. *Physics Today*, 22(2):80–80, 1969.

[11] J. Preskill. *Lecture Notes for Physics 229:Quantum Information and Computation*. CreateSpace Independent Publishing Platform, 2015.

[12] J.F. Clauser, M.A. Horne, A. Shimony, and R.A. Holt. Proposed experiment to test local hidden-variable theories. *Physical Review Letters*, 23(15):880–884, 1969.

[13] Jan-Åke Larsson. Loopholes in bell inequality tests of local realism. *Journal of Physics A: Mathematical and Theoretical*, 47(42):424003, oct 2014.

[14] Alain Aspect, Jean Dalibard, and Gérard Roger. Experimental test of bell's inequalities using time-varying analyzers. *Phys. Rev. Lett.*, 49:1804–1807, Dec 1982.

[15] Alain Aspect, Philippe Grangier, and Gérard Roger. Experimental realization of einstein-podolsky-rosen-bohm gedankenexperiment: A new violation of bell's inequalities. *Phys. Rev. Lett.*, 49:91–94, Jul 1982.

[16] Serge Massar, Stefano Pironio, Jérémie Roland, and Bernard Gisin. Bell inequalities resistant to detector inefficiency. *Phys. Rev. A*, 66:052112, Nov 2002.

[17] E. Zambrini Cruzeiro and N. Gisin. Complete list of tight bell inequalities for two parties with four binary settings. *Phys. Rev. A*, 99:022104, Feb 2019.

[18] Philippe H. Eberhard. Background level and counter efficiencies required for a loophole-free einstein-podolsky-rosen experiment. *Phys. Rev. A*, 47:R747–R750, Feb 1993.

[19] Marissa Giustina, Marijn A. M. Versteegh, Sören Wengerowsky, Johannes Handsteiner, Armin Hochrainer, Kevin Phelan, Fabian Steinlechner, Johannes Kofler, Jan-Åke Larsson, Carlos Abellán, Waldimar Amaya, Valerio Pruneri, Morgan W. Mitchell, Jörn Beyer, Thomas Gerrits, Adriana E. Lita, Lynden K. Shalm, Sae Woo Nam, Thomas Scheidl, Rupert Ursin, Bernhard Wittmann, and Anton Zeilinger. Significant-loophole-free test of bell's theorem with entangled photons. *Phys. Rev. Lett.*, 115:250401, Dec 2015.

[20] Lynden K. Shalm, Evan Meyer-Scott, Bradley G. Christensen, Peter Bierhorst, Michael A. Wayne, Martin J. Stevens, Thomas Gerrits, Scott Glancy, Deny R. Hamel, Michael S. Allman, Kevin J. Coakley, Shellee D. Dyer, Carson Hodge, Adriana E. Lita, Varun B. Verma, Camilla Lambrocco, Edward Tortorici, Alan L. Migdall, Yanbao Zhang, Daniel R. Kumor, William H. Farr, Francesco Marsili, Matthew D. Shaw, Jeffrey A. Stern, Carlos Abellán, Waldimar Amaya, Valerio Pruneri, Thomas Jennewein, Morgan W. Mitchell, Paul G. Kwiat, Joshua C. Bienfang, Richard P. Mirin, Emanuel Knill, and Sae Woo Nam. Strong loophole-free test of local realism. *Phys. Rev. Lett.*, 115:250402, Dec 2015.

[21] B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. L. Vermeulen, R. N. Schouten, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, M. Markham, D. J. Twitchen, D. Elkouss, S. Wehner, T. H. Taminiau, and R. Hanson. Loophole-free bell inequality violation using electron spins separated by 1.3 kilometres. *Nature*, 526:682 EP –, 10 2015.

[22] Johannes Kofler, Marissa Giustina, Jan-Åke Larsson, and Morgan W. Mitchell. Requirements for a loophole-free photonic bell test using imperfect setting generators. *Phys. Rev. A*, 93:032115, Mar 2016.

[23] J. Aron. Ibm unveils its first commercial quantum computer. https://www.newscientist.com/article/2189909-ibm-unveils-its-first-commercial-quantum-computer/.

[24] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. Quantum cryptography. *Rev. Mod. Phys.*, 74:145–195, Mar 2002.

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

[26] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, 560:7 – 11, 2014. Theoretical Aspects of Quantum Cryptography – celebrating 30 years of BB84.

[27] Artur K. Ekert. Quantum cryptography based on bell's theorem. *Phys. Rev. Lett.*, 67:661–663, Aug 1991.

[28] Charles H. Bennett, Gilles Brassard, and N. David Mermin. Quantum cryptography without bell's theorem. *Phys. Rev. Lett.*, 68:557–559, Feb 1992.

[29] Gilles Brassard, Norbert Lütkenhaus, Tal Mor, and Barry C. Sanders. Limitations on practical quantum cryptography. *Phys. Rev. Lett.*, 85:1330–1333, Aug 2000.

[30] Dominic Mayers and Andrew Yao. Quantum cryptography with imperfect apparatus. In *Proceedings of the 39th Annual Symposium on Foundations of Computer Science*, FOCS '98, pages 503–, Washington, DC, USA, 1998. IEEE Computer Society.

[31] Jonathan Barrett, Lucien Hardy, and Adrian Kent. No signaling and quantum key distribution. *Phys. Rev. Lett.*, 95:010503, Jun 2005.

[32] Reinhold A Bertlmann and Anton Zeilinger. *Quantum [Un]Speakables II, half a century of Bell's Theorem.* Frontiers collection. Springer, Switzerland, 2017.

[33] V. B. Braginskii and Iu. I. Vorontsov. Quantum-mechanical limitations in macroscopic experiments and modern experimental technique. *Uspekhi Fizicheskikh Nauk*, 114:41–53, Sep 1974.

[34] C. K. Hong, Z. Y. Ou, and L. Mandel. Measurement of subpicosecond time intervals between two photons by interference. *Phys. Rev. Lett.*, 59:2044–2046, Nov 1987.

[35] Agata M. Brańczyk. Hong-Ou-Mandel Interference. *arXiv e-prints*, page arXiv:1711.00080, Oct 2017.

[36] Joseph B. Altepeter, Daniel F.V. James, and Paul G. Kwiat. *4 Qubit Quantum State Tomography*, pages 113–145. Springer Berlin Heidelberg, Berlin, Heidelberg, 2004.

[37] Paul G. Kwiat, Klaus Mattle, Harald Weinfurter, Anton Zeilinger, Alexander V. Sergienko, and Yanhua Shih. New high-intensity source of polarization-entangled photon pairs. *Phys. Rev. Lett.*, 75:4337–4341, Dec 1995.

[38] M. Arcari, I. Söllner, A. Javadi, S. Lindskov Hansen, S. Mahmoodian, J. Liu, H. Thyrrestrup, E. H. Lee, J. D. Song, S. Stobbe, and P. Lodahl. Near-unity coupling efficiency of a quantum emitter to a photonic crystal waveguide. *Phys. Rev. Lett.*, 113:093603, Aug 2014.

[39] Paul G. Kwiat and Harald Weinfurter. Embedded bell-state analysis. *Phys. Rev. A*, 58:R2623–R2626, Oct 1998.

[40] Karen Hecht, Eugene;Lippert. *Optics.* De Gruyter, Inc, Berlin/Boston, 2018.

[41] H. Sanabria and B.M. RodrÃguez Lara. An introduction to quantum interferometry: Young's experiment with fock and coherent states. *Revista mexicana de fisica E*, 53:97 – 105, 06 2007.

[42] J. Calsamiglia and N. Lütkenhaus. Maximum efficiency of a linear-optical bell-state analyzer. *Applied Physics B*, 72(1):67–71, Jan 2001.

[43] Daniel F. V. James, Paul G. Kwiat, William J. Munro, and Andrew G. White. Measurement of qubits. *Phys. Rev. A*, 64:052312, Oct 2001.

[44] Fosco connect. Optical fiber loss and attenuation. http://www.fiberoptics4sale.com/wordpress/optical-fiber-loss-and-attenuation/.

[45] Peter Lodahl. Quantum-dot based photonic quantum networks. *Quantum Science and Technology*, 3(1):013001, oct 2017.

[46] Thorlabs. Choosing a waveplate. www.thorlabs.de/newgrouppage9.cfm?objectgroup_id=10777, 2019.

[47] Marco Ornigotti, Lukas Maczewsky, and Alexander Szameit. Fundamentals of quantum optics - lecture notes. *Friedrich-Schiller Universität - Jena*, 2016.

[48] Yu He, Yu-Ming He, Y.-J. Wei, X. Jiang, M.-C. Chen, F.-L. Xiong, Y. Zhao, Christian Schneider, Martin Kamp, Sven Höfling, Chao-Yang Lu, and Jian-Wei Pan. Indistinguishable tunable single photons emitted by spin-flip raman transitions in ingaas quantum dots. *Phys. Rev. Lett.*, 111:237403, Dec 2013.

[49] N. Prtljaga, C. Bentham, J. O'Hara, B. Royall, E. Clarke, L. R. Wilson, M. S. Skolnick, and A. M. Fox. On-chip interference of single photons from an embedded quantum dot and an external laser. *Applied Physics Letters*, 108(25):251101, 2016.

[50] N. Somaschi, V. Giesz, L. De Santis, J. C. Loredo, M. P. Almeida, G. Hornecker, S. L. Portalupi, T. Grange, C. Antón, J. Demory, C. Gómez, I. Sagnes, N. D. Lanzillotti-Kimura, A. Lemaítre, A. Auffeves, A. G. White, L. Lanco, and P. Senellart. Near-optimal single-photon sources in the solid state. *Nature Photonics*, 10:340 EP –, 03 2016.

[51] Xing Ding, Yu He, Z.-C. Duan, Niels Gregersen, M.-C. Chen, S. Unsleber, S. Maier, Christian Schneider, Martin Kamp, Sven Höfling, Chao-Yang Lu, and Jian-Wei Pan. On-demand single photons with high extraction efficiency and near-unity indistinguishability from a resonantly driven quantum dot in a micropillar. *Phys. Rev. Lett.*, 116:020401, Jan 2016.

[52] R. Stockill, M. J. Stanley, L. Huthmacher, E. Clarke, M. Hugues, A. J. Miller, C. Matthiesen, C. Le Gall, and M. Atatüre. Phase-tuned entangled state generation between distant spin qubits. *Phys. Rev. Lett.*, 119:010503, Jul 2017.