UNIVERSITY OF COPENHAGEN
NIELS BOHR INSTITUTE

Single-photon sources as a key resource for developing a global quantum network

Ph.D. Thesis

Submitted on
January 14th (2023)

Eva M. González Ruiz
Supervised by Prof. Anders S. Sørensen

Single-photon sources as a key resource for developing a global quantum network

Author Eva M. González-Ruiz
Advisor Prof. Anders S. Sørensen

UNIVERSITY OF COPENHAGEN
FACULTY OF SCIENCE

Theoretical Quantum Optics Group
Center for Hybrid Quantum Networks (Hy-Q)
Niels Bohr Institute

This thesis has been submitted to
the PhD School of SCIENCE, University of Copenhagen,
in partial fulfillment of the requirements
for the degree of Doctor of Philosophy

January 17, 2023

Single-photon sources as a key resource for developing a global quantum network

Ph.D. Thesis

University of Copenhagen, 14$^{\text{th}}$ of January 2023

To my sister, for always inspiring me
with your strong will, resilience and warm heart.

Abstract

The development of the global quantum internet has progressed significantly in the recent years. It requires the simultaneous progress of very diverse quantum platforms, which thus entitles multitude of different challenges both theoretically and experimentally. In this thesis we approach several of these tasks by proposing single-photon sources as an important resource that provides with many valuable solutions, from an efficient loophole-free violation of Bell's inequality (González-Ruiz et al., 2022a) to optimal implementations of Device-Independent Quantum Key Distribution protocols (González-Ruiz et al., 2022b). To this end we introduce a detailed analysis that model realistic imperfections of the sources (Bjerlin et al., 2023; González-Ruiz et al., 2022a), in order to reach a deeper understanding that allows us to set a clearer route for near-future experimental implementations. In addition, we present a full theoretical analysis (González-Ruiz et al., 2023) of the path-entangled states experimentally realised by Østfeldt et al. (2022) by means of a quantum-dot biexciton cascade placed in a chiral nanowaveguide, investigating their entanglement properties after the effect of several realistic imperfections. Finally, we propose an experimental set-up to match the typical broad bandwidth of photons generated by quantum-dot single-photon sources with that of quantum memories candidates such high-Q optomechanical membranes, with a bandwidth several orders of magnitude narrower. Our proposal allows thus to efficiently store the qubit carried by the photon.

Dansk resumé

Udviklingen af det globale kvanteinternet har set markante fremskridt de seneste år. Det kræver den samtidige udvikling af mange forskellige kvanteplatforme, som dermed bringer mange forskellige udfordringer, både teoretiske og eksperimentelle, med sig. Denne afhandling undersøger vi flere af disse udfordringer ved at foreslå enkeltfotonkilder som en vigtig ressource, der giver mange værdigfulde løsninger, lige fra en effektiv smuthulfri krænkelse af Bells ulighed (González-Ruiz et al., 2022a) til optimale implementeringer af Device-Independent Quantum Key Distribution protokoller (González-Ruiz et al., 2022b). Til dette formål introducere vi en detaljeret analyse der modellerer realistiske ufuldkommenheder af kilderne (Bjerlin et al., 2023; González-Ruiz et al., 2022a), for at opnå en dybere forståelse, der giver os mulighed for at sætte en klarere for nær-fremtidige eksperimentelle implementeringer. Derudover præsentere vi en fuldstændig teoretisk analyse (González-Ruiz et al., 2023) at de vej-entanglede tilstande eksperimentelt realiseret af Østfeldt et al. (2022) ved hjælp af en kvante-dot biexciton-kaskade placeret i en chiral nanowaveguide, der undersøger deres entanglement-egenskaber påvirkning af flere realistiske fejlkilder. Endelig foreslår vi et eksperimentielt set-up til at tilpasse den typiske brede båndbredde af fotonerne genereret af en kvante-dot-enkeltfotonkilde med kvantehukommelseskandidaten høj-Q optomekaniske membraner, med en flere størrelsesordner smallere båndbredde, med målet om at kunne være i stand til effektivt at lagre kvante-bits båret af fotoner.

Acknowledgments

The world has deeply changed in the last three years. If I have been able to navigate this strange but also exciting time as Ph.D. student is thanks to many fantastic people. To all of you, mentioned below or unforgivably forgotten, thanks from the bottom of my heart.

I would like to start by thanking my supervisor, Anders Sørensen. Maybe people start by thanking their principal supervisors because they feel they must. In my case I truly feel obliged to express how important for me you have been during this time, both as the wonderful mentor, cheerful teacher and understanding boss you were when things got really hard. Your love for physics is contagious, and so is your sense of fairness and kindness (specially appreciated in your debut as section leader). I feel very lucky to have spent the last five and a half years learning from you.

I would like to continue by acknowledging Toni Acín, for hosting me in the Quantum Information Theory group during my external stay at ICFO, in Barcelona. I really had a wonderful time there, where I certainly learned a lot of new physics and met amazing colleagues and new friends. I feel very thankful for the opportunity and I look forward to keep on collaborating in the future.

I also want to thank all of you I have had the privilege of collaborating with during these years. Thanks to Freja, for your infinite patience and so many helpful discussions; to Johannes, always getting a smile out of everyone; Mads, also for all your moral support (and final proofreadings!); Sumanta, in the very beginning of the Ph.D., always appreciated your efforts in gluing the group together; Enky and Javier, my partners-in-crime at ICFO (specially thanks to Javier for all the Barcelona F.C. gifts I was forced to accept at the group's secret santa). I would further like to thank Peter Lodahl, Leonardo Midolo, Ravitej Uppu and Albert Schliesser for all the fruitful discussions during these years. I have learned insanely much from all of you.

I feel very grateful for having spent my time at such an enriching place as Hy-Q and, specially, the Theoretical Quantum Optics group. It really feels like a family, and thanks to it I have met amazing colleagues and truly friends. Thanks to the (clearly) best office mates in the whole NBI, for helping me keep sane and feel more like home during working hours: Johann, Ying, Vasso, Cecilie, Ming Lai and Evi. Our sofa will be a legacy thanked by many future student generations. I also want to thank my bimbo friend Camille for all the supportive conversations and backing during this time. I would further like to thank the Unresolved Sideband for rocking it year after year. Thanks for giving me the opportunity of joining you! Finally, thanks to all the wonderful members of the npn. You all really made my time at NBI unforgettable.

Thanks to all my SymfUni family, who has made Denmark feel truly like a home. Thanks to my roommate and brother-from-different-parents Raúl. The lockdown was infinitely better with your positivity and optimism (also with our contemporary cooking experiments and terrace-farming attempts, of course). Very warm thanks to all my friends back home: the NYG, with whom it feels like time has not gone by every time we see each other; and specially María, you were always there when I needed you.

To my big family, you are the rock that I always know I can turn to when things get really difficult (and they did). I want to thank my grandma for her daily morning message, that helped me start even the worst days with a smile. Thanks to my parents and sister, whom I feel always close regardless of how far Madrid is from little Copenhagen. Thanks to you I made it this far, and there are no words to express how grateful I feel for having you in my life.

I would really like to thank my partner Anton, for so much that it is a bit complicated to summarize. A brilliant physics mate, my best friend and my strongest, unconditional support during this time. I could not have made it without you.

Finally, I want to remember those I did not have the chance to say a proper goodbye to in the spring of 2020. The world is indeed very different compared to three years ago, specially without you. Thank you for believing in me.

List of publications

- **Eva M. González-Ruiz**, Sumanta K. Das, Peter Lodahl, and Anders S. Sørensen (2022). *Violation of Bell's inequality with quantum-dot single-photon sources*. In: *Phys. Rev. A* 106 (1), p. 012222. DOI: 10.1103/PhysRevA.106.012222
- Freja T. Østfeldt, **Eva M. González-Ruiz**, Nils Hauff, Ying Wang, Andreas D. Wieck, Arne Ludwig, Rüdiger Schott, Leonardo Midolo, Anders S. Sørensen, Ravitej Uppu, and Peter Lodahl (2022). *On-Demand Source of Dual-Rail Photon Pairs Based on Chiral Interaction in a Nanophotonic Waveguide*. In: *Phys. Rev. X Quantum* 3 (2), p. 020363. DOI: 10.1103/PRXQuantum.3.020363
- **Eva M. González-Ruiz**, Javier Rivera-Dean, Marina F. B. Cenni, Anders S. Sørensen, Antonio Acín, and Enky Oudot (2022). *Device Independent Quantum Key Distribution with realistic single-photon source implementations*. DOI: 10.48550/ARXIV.2211.16472. Submitted to *Quantum*.
- **Eva M. González-Ruiz**, Freja T. Østfeldt, Ravitej Uppu, Peter Lodahl, and Anders S. Sørensen (2023). *Entanglement properties of a quantum-dot biexciton cascade in a chiral nanophotonic waveguide*. DOI: 10.48550/arXiv.2301.04444. Submitted to *Phys. Rev. A*.
- Johannes Bjerlin, **Eva M. González-Ruiz**, and Anders S. Sørensen (2023). *Two photon correlations for a quantum-dot single photon source*. In preparation.

Contents

Abstract **i**

Dansk resumé **iii**

Acknowledgments **v**

List of publications **vii**

Introduction: towards the quantum internet **1**
I. Quantum information sources . . . 2
II. A safe quantum network . . . 7
III. Storing the quantum information . . . 13
Structure of the thesis . . . 14

1 Violation of Bell's inequality with quantum-dot single-photon sources **15**
1.1 Introduction . . . 15
1.2 Ideal implementation . . . 17
1.3 Model for real sources . . . 19
1.3.1 Dephasing . . . 20
1.3.2 Optical loss . . . 22
1.3.3 Purity . . . 23
1.4 Analysis . . . 24
1.4.1 Effect of distinguishability of photons . . . 26
1.4.2 Losses and multi-photon errors . . . 28
1.4.3 Optimizing the probability of transmission T . . . 32
1.4.4 Memory considerations . . . 35
1.5 Conclusion and outlook . . . 35

2 Two-photon correlations for a quantum dot single-photon source **37**
2.1 Introduction . . . 37
2.2 Analysis . . . 38
2.2.1 HOM Visibility . . . 39
2.2.2 Bounds on the relation between HOM visibility and purity . . 41

2.3 Results 44
2.4 Conclusions and Outlook 46

3 Entanglement properties of a quantum-dot biexciton cascade in a chiral nanophotonic waveguide 47
3.1 Introduction 47
3.2 Analysis 50
3.2.1 The Hamiltonian and wavefunction ansatz 50
3.2.2 Solving the Schrödinger equation 55
3.2.3 Entanglement generation 57
3.3 Results 59
3.3.1 Fine-structure splitting 60
3.3.2 Imperfect chirality 61
3.3.3 Timing jitter 62
3.3.4 Asymmetric exciton decay 64
3.4 Conclusion 65

4 New key-rate lower bounds for DIQKD implementations with single-photon sources 67
4.1 Introduction 67
4.2 Experimental setup 70
4.3 DIQKD protocol 73
4.4 Results 75
4.4.1 Comparison with analytical formulas 75
4.4.2 Dependence of the key rate on the distinguishability of the generated photons 77
4.4.3 Dependence of the key rate on the purity of the generated state 78
4.4.4 Finite size analysis 80
4.5 Conclusion 82

5 The single-photon stretcher 85
5.1 Introduction 86
5.2 Analysis 87
5.2.1 Single-mode contribution 89
5.2.2 Multi-mode contribution 93
5.2.3 Crossed terms 96
5.2.4 Total contribution 97
5.3 Conclusion and next steps 98

Final remarks 99
Conclusion 99
Outlook 100

Appendix 103

A Appendix to Chapter 1 **103**
A.1 Dephasing in single-photon emitters 103
A.2 Photon operator transformations 106
A.3 Conditioning on the correct detection pattern 107
A.4 Probability events P_{ijkl} 109

B Appendix to Chapter 4 **111**
B.1 Equivalence between the assignment strategy in CHSH and Eberhard's inequality 111
B.2 Modelling of real single-photon sources and detectors 112
B.3 Numerical implementation 115
B.3.1 Optimization of the experimental parameters 115
B.3.2 SDP relaxation 116
B.3.3 Parallelization 117

Bibliography **119**

List of Figures

1 a) STM image of a InGaAs QD. b) Level structure of a InGaAs QD. . 5
2 A possible scheme of the quantum internet implementation. 8
3 Diagram with relations between Alice's and Bob's entropies 12

1.1 a) Set-up proposed in Kołodyński et al. (2020), consisting of two local stations (Alice and Bob) and a central heralding station (CHS). b) Example of quantum-dot single-photon source and its energy level schemes. 17
1.2 Degree of indistinguishability of photons from different sources, i.e. the HOM visibility $V_\beta^{(0)}$. 20
1.3 Sketch of the efficiencies η_i and definitions of the creation operators of the lost photons $\hat{c}^\dagger$. 23
1.4 a) Violation of the CHSH inequality $S \geq 2$, as a function of the HOM visibility of the local sources $V_\alpha^{(0)}$. b) Contour plot of the CHSH value S as a function of the visibilities V_α and V_β. 25
1.5 Evaluation of CHSH threshold for a postselected protocol and with finite multi-photon contributions. 28
1.6 CHSH parameter S as a function of the local efficiency η_l of Alice and Bob's stations for different HOM visibilities. 31
1.7 Threshold for the violation of the CHSH Bell's inequality ($S \leq 2$). . . 32
1.8 Effect of finite transmittance T. a) CHSH parameter S as a function of the transmittance T of the beam-splitters at the end stations for several sets of single-source error parameters. b) Number of standard deviations Z' with which a violation of Bell's inequality is achieved as a function of the transmittance T. 33

2.1 HOM visibility of QD in a leaky waveguide with phase shift $\theta = \pi/2$, at different pulse lengths, plotted against the corresponding value of $g_p^{(2)}$. 44
2.2 Factor $F = (1 - V)/g^{(2)}$ at different pulse lengths. 45

3.1 Entanglement generation scheme and level structure of the quantum dot (QD). 48

3.2 Time correlations P_{AA} and P_{AB} as a function of the difference in the emission time τ. 59
3.3 a) Time correlations P_{AA}, P_{AB}, P_{BA}, P_{BB} as a function of the difference in the emission time τ. b) Colour map of the concurrence C of the state as a function of the difference in phase Φ and the difference in emission times τ. 60
3.4 a) Concurrence C of the state as a function of the detection timing jitter for several values of chirality Φ and time difference τ. b) Concurrence C of the state for different degree of chirality, quantified by the phase Φ. c) Corresponding probability density $\bar{N}$ of the detection time for the situation analysed in (b). 63
3.5 a) Concurrence C of the state as a function of the time delay τ at different degrees of the chirality, quantified by Φ. b) Colour map of the concurrence of the state as a function of the difference in phase Φ and the time τ for $\epsilon = -0.4$. 65

4.1 Heralded set-up introduced in Ref. (Kołodyński et al., 2020). 70
4.2 Measurement set-up in Alice's station. 71
4.3 Dependence of the key rate on the detection efficiency η_l for the case of $V_{\mathrm{HOM}} = 1.0$ and $g^{(2)} = 0$. 76
4.4 Dependence of the key rate on the visibility V_{HOM}. 78
4.5 Dependence of the key rate on the autocorrelation function $g^{(2)}$ in log scale. 79
4.6 Key rate in bits per second as a function of the distance. 80

5.1 Artist's impression of the single-photon stretcher. Credits: Elena González Ruiz (2022). 85
5.2 Scheme of the photon stretcher set-up. 88
5.3 (a) Plot of the different wavefunctions involved in the optimisation of the number of single-mode cavity photons. (b) Normalisation of the different wavefunctions plotted in (a) 92

B.1 CHSH parameter S as a function of the local efficiency η_l of Alice and Bob's stations for different HOM visibilities optimized with respect to the transmittance t. 114
B.2 HSH parameter S as a function of the local efficiency η_l of Alice and Bob's stations for different purities and HOM visibilities optimized with respect to the transmittance t. 114
B.3 Schematic representation of our numerical implementation. 116
B.4 Key rate for $V = 0.95$ computed with two different values of m: $m = 2$ and $m = 8$. 117

List of Tables

1.1 Different contributions to the probabilities $P(A = x, B = y)$, $P(A = x, B = \emptyset)$, $P(A = \emptyset, B = y)$ and $P(A = \emptyset, B = \emptyset)$. 29

4.1 Probability contributions to the total probability of detection $p(a_i, b_i|x_i, y_i)$. 72

A.1 4-photon and 5-photon events that lead to a correct detection pattern at the CHS. 110

Introduction: towards the quantum internet

In the recent years the quantum physics community has witnessed an increasing interest towards the development of quantum technologies (McKinsey&Company, 2021). These technologies have progressively attracted the interest of the biggest multinational technology companies and worldwide economic powers' short and long-term investing plans. This enthusiasm has in many cases smoothly developed into a competition towards a hyped first-come, first served quantum prize (Candelon et al., 2022). Such prize has very different forms in the context of quantum technologies, and ranges from the first quantum computer to claim quantum advantage (Arute et al., 2019), a pioneer quantum simulator that could create breakthroughs in the pharmaceutical industry or contribute to explore fundamental science not reachable before (Daley et al., 2022), a quantum metrology system that could approach the very limits of measurement precision (LIGO Scientific Collaboration and Virgo Collaboration et al., 2016; Zhao et al., 2020; McCuller et al., 2020), to the first global network for quantum communications (Wehner et al., 2018; Lu et al., 2021). The latter could be extended to an actual quantum internet infrastructure (Kimble, 2008) that allows for safer and more efficient exchange of information, in times where this is more important than ever.

The development of both a mature and realistic quantum internet requires the close collaboration of many different disciplines: new algorithms, hardware, control and theoretical modelling are needed in the process (European Quantum Flagship, 2022). All of which can be assigned to different building blocks that constitute the structure of the quantum internet, each addressed separately though with the same common goal.

Each of the chapters in this thesis will deal with a few of these building blocks. We explore a few of the current challenges withing some of the research areas and contribute in complementary ways to the development of the quantum internet. In this introductory chapter we aim to present and contextualise the essential concepts that will be of use for the subsequent chapters, as well as the main motivation and story behind the different projects. This broader motivation glues the smaller pieces of research presented in this thesis together towards the common purpose of contributing to the development of a global and safe universal quantum network.

I. Quantum information sources

The first step towards designing any communication and processing network is to establish how to actually generate each of the smaller "chunks" in which we plan of splitting the information. While classical computing uses the *bit* (a unit of information consisting either on a 0 or a 1), quantum processing systems encode the information in *qubits*. These quantum units of information are a more advanced resource than their classical counter parts. In fact, the mathematical description of a qubit requires a $\mathbb{C}^2$ number[1].

So what is special about using qubits as the information units in our network? The two main resources that quantum units of information can provide with, compared to classical bits, are *superposition* and *entanglement*. The first one is an intrinsic property of quantum systems that allows for preparing the qubit in neither only the "0" or "1" state, but actually both simultaneously. An example of such a state is the even superposition

$$|\psi\rangle = \frac{1}{\sqrt{2}}(\,|0\rangle + |1\rangle\,)\,. \tag{1}$$

An entangled state is that which can not be expressed as a product of its constituents (in which case is called a product state). In other words, if an entangled state is shared among several parties, it is impossible to describe it fully as the composition of each of the bits owned by them individually. Mathematically, an entangled state ρ can never be expressed as $\sum_i p_i \rho_{A,i} \otimes \rho_{B,i}$, where $\rho_{A,i}$ and $\rho_{B,i}$ are the corresponding states of the individual parties and p_i are positive valued probabilities. An example of entangled states are the four Bell states

$$\left|\psi^{\pm}\right\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle \pm |10\rangle\right), \quad \left|\phi^{\pm}\right\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle \pm |11\rangle\right), \tag{2}$$

which form a complete basis of the two-qubit Hilbert space.

Both the superposition and entanglement of qubits constitute the very basic fuel of any achievable advantage by means of quantum processing. These special properties come however at a price. Unfortunately[2] these properties arise at a scale size way smaller than that we live in: the nanometer scale. In fact, one of the initial motivations for the quantum computing research was the foreseen end of the empirical Moore's law (Moore, 1998), when transistors reach such a small size that the physical laws governing its design up to that point are no longer applicable. Once the nano-meter scale is reached, the physical laws governing are those from quantum mechanics. One thus needs to find a new suitable platform to carry the units of information, and such source of information must live in the mentioned smalled length scale.

[1] This, however, could lead to the misleading interpretation that the benefits of quantum mechanics could be just as fine simulated only by real numbers. This assertion was recently proven wrong in Renou et al. (2021).

[2] or fortunately, though?

This is nevertheless not the only requirement. A platform for qubits must of course be accessible for us macroscopic creatures in some relatively easy way, if we aim to control these features for information processing. We need physical systems that can be sufficiently well manipulated and measured despite their small size. This also imposes restrictions regarding how good the qubit platform is at interacting with other qubits in a deterministic and controllable way, and with how much certainty would one be able to read out its state. Once these challenges are overcome, one must also ensure that the interaction of the qubit with its environment is sufficiently low such that the encoded information is not contaminated or lost during its processing. This is what is known as a *decoherence* process, and is one of the main challenges in any quantum information hardware. Other features of the source of qubits of choice that are also of high relevance, specially for communication purposes, are the rate at which they can be generated, their fidelity (this is, how similar the qubit actually created is to the one that ideally wanted to generate), and how easy would it be to produce and use them at a large scale in the future.

Despite all the hard conditions to be complied with, there are several strong candidates to perform as a source of qubits. There is, however, always a compromise between their compared features: for example, some qubit platforms may almost perfectly suitable regarding most requirements, however suffering from a difficult prospect of large-scale integration. This is the case of the first realisation of qubits, performed by means of *ion traps* as first proposed in Cirac et al. (1995) and, for instance, experimentally utilised for quantum simulation in Zhang et al. (2017). Other successful candidates are *superconducting qubits*, with great control and measurement possibilities but stronger interactions with their solid state environment makes them more susceptible to decoherence processes (Kjaergaard et al., 2020; Arute et al., 2019); *topological qubits*, that use topological protection against decoherence but that have been however highly challenging to produce and manipulate up to date (Aghaee et al., 2022); the spin degree of freedom in *quantum dots* (Chan et al., 2022; Hendrickx et al., 2020), whose ability to generate single photons will be widely described in the following sections; and *nitrogen-vacancy (NV) centers* (Wang et al., 2020) can also constitute a promising solid-state qubit and, finally, *photonic qubits* (see for example Takeda et al. (2019) for continuous variable implementations or Uppu et al. (2021a) and Slussarenko et al. (2019) for discrete variables). Photons suffer from very little decoherence as (provided their frequency is chosen suitably) they can propagate through air or optical fibers almost without interacting with their surroundings and are easily measured by means of photodetecting devices. Their low interaction also results in their main flaw, since qubit-qubit interactions exclusively by means of photons is not achievable without light-matter interaction (Gorshkov et al., 2011; Li et al., 2021).

The work of this thesis is mostly focused on sources of photonic qubits, aiming towards a photonic realisation of the quantum internet. In the following subsections we introduce both the sources needed for generating single photons and entangled states of photons.

Single-photon sources

If we want to encode quantum information in photons, the light generated by everyday light sources such as light bulbs and LEDs is ill-suited as it can not manifest the quantum features that we are interested in. We need to use one and only one photon at a time, to pursue such processing. In fact defining what a single photon actually means is not that simple. We can not have a space-localised photon of a single frequency, or vice-versa, as this would violate Heisenberg's uncertainty principle. One then rather defines a single photon as either having a very narrow frequency bandwidth or as a superposition of several monochromatic photons. In other words, a single photon is one partially space-time localised excitation of the electromagnetic field (Eisaman et al., 2011).

Generating one and only one photon at a time is not a trivial task. Photons per se are a good qubit platform and satisfy most of the requirements exposed above. They are nevertheless required to also have certain characteristics, which will rely on the single-photon source generating them. In particular, the single-photon source (SPS) needs to be able to generate indistinguishable photons: that is, photons that can not be differentiated through any of their features. The source must also be highly pure, which means that not more than one single-photon is released at a time, and efficient, so that photons are emitted with high probability upon the excitation of the source. As any other quantum source of qubits, the SPS should also be able to generate them at a high rate and be easily scalable to large-scale production.

There are two main types of SPS: on-demand and heralded sources. Heralded or probabilistic sources consist of those which in fact emit a pair of photons with a certain probability, but which can be used as a SPS by detecting one of the photons of the pair as an indication that the generation process indeed succeeded. These sources can be excited at very high rates, but the probability of successful heralding events is lower than other on-demand sources. The main examples of heralded SPS are based on non-linear processes and are Spontaneous Parametric Down-Conversion (SPDC) sources (Harris et al., 1967; Magde et al., 1967), which generates pairs of entangled photons, and the less extended Four-Wave Mixing (FWM) sources (Fan et al., 2007). On-demand or deterministic SPS, on the other hand, generate single photons by means of a non-probabilistic process that succeeds up to a certain efficiency, typically leading to a higher single-photon emission rate. They are usually based on a two-level system that emits a photon after being excited. Some deterministic single-photon sources involve molecules (Lounis et al., 2000), the aforementioned NV centers (Babinec et al., 2010), Rydberg atoms (Ripka et al., 2018) or quantum dots (QD) (Uppu et al., 2020).

In this thesis we analyse in depth the performance of quantum-dot single-photon sources for various applications. In particular, we focus on InGaAs self-assembled QDs (see Fig. 1). With respect to the required characteristics explained above, InGaAs QDs are highly proficient, since the indistinguishability of the generated photons has been shown to be up to 96% and their purity has been measured to

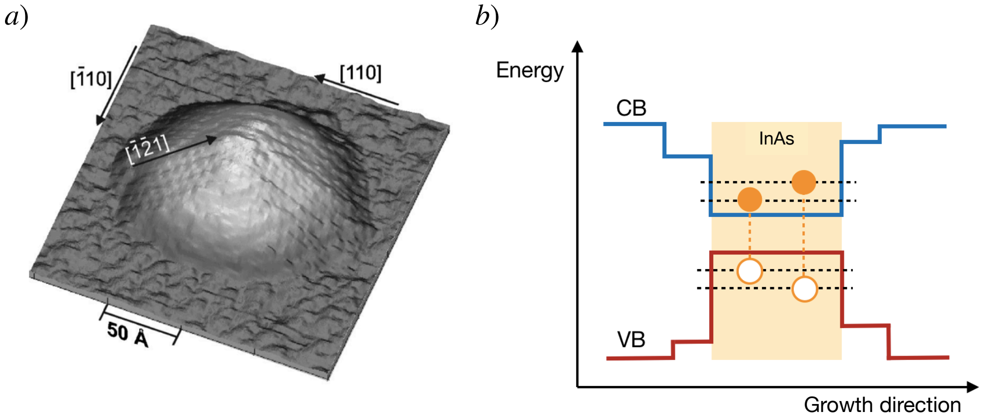


Figure 1: a) STM image of a InGaAs QD (Source: Márquez et al. (2001)). b) Level structure of a InGaAs QD. The valence band (in red) and the conduction band (in blue) are modified with the insertion of the InAs layer, creating an effective atomic level structure for the electrons (orange dots) and holes (white dots) (Source: González-Ruiz (2018)).

be up to 99.4%[3] (Tomm et al., 2021; Uppu et al., 2020). These QDs are obtained by means of InAs embedded in GaAs layers, that due to the lattice mismatch between the two, randomly generates QDs on the surface by strain in a method called Stranski-Krastanov growth (Stranski et al., 1937). The difference in potential between the two materials creates an effective two level system between the valence and conduction bands for the electrons and holes (see Fig. 1b). Thus, the QDs behave like artificial atoms despite being solid state systems, therefore with the same capability of emitting single photons upon excitation and relaxation. Depending on the excitation process and the bias voltage[4] applied to the QD, there will be one or more electrons upgraded from the valence to the conduction band. If two electron-hole pairs are created, the state is known as *biexciton* ($|XX\rangle$), while a single pair constitutes an *exciton* ($|X\rangle$). Each of the states have different spin properties that dictate the allowed transitions to lower energy states (Lodahl et al., 2015). The exciton state is typically used to emulate a two level system, and thus widely used for generating single photons. The biexciton state, on the other hand, generates a pair of entangled photons, and will be one of the entanglement sources introduced in the following subsection.

In **Chapter 1** we introduce a model for realistic quantum-dot single-photon sources that allows us to analyse their indistinguishability, purity and efficiency in connection with their usual decoherence mechanisms. Although the goal of the chapter is to analyse those characteristics of the single-photon sources in order to perform a higher violation of Bell's inequality, this model is completely general and

[3] A detailed model for realistic quantum-dot single-photon sources and how the related imperfections can affect their required properties is introduced in **Chapter 1**.

[4] A constant voltage is typically applied to tune the QDs such that electrons from the solid state environment do not affect the intended level structure (Østfeldt, 2020).

applicable for analysis the performance of other protocols or simply understanding better the limitations of quantum-dot single-photon sources. Furthermore, **Chapter** 2 explores the connection between the indistinguishability of photons and the purity of the single-photon source that originated them.

Entanglement sources

We have already mentioned that entanglement is one of the main resources that quantum systems provide with in order to outperform classical information protocols (Jozsa et al., 2003). Therefore the ability to generate entangled states is a very important requirement towards the development of the quantum internet. There has been developed many different approaches to the generation of entangled states throughout the years, and similarly to the challenging generation of single photons, each of the proposals has stronger and weaker characteristics.

The entanglement source of choice will also depend on the type of qubit to be entangled. Creating entanglement by measurement is for example of great utility for entangling distant atoms or atomic ensembles (see Bose et al. (1999) or Duan et al. (2001) for the DLCZ protocol). Photonic entangled states, on the other hand, can be generated probabilistically by means of different linear optics set-ups, however with a maximum probability of success of 50% (Calsamiglia et al., 2001). This can quickly become an issue, if a protocol requires the simultaneous generation of many entangled states. Similarly, the aforementioned probabilistic SPDC sources can be used as entangled-state sources instead of single-photon sources, as the emitted photon pairs from the non-linearity are entangled (Zhong et al., 2018). For instance, the idea of entanglement swapping (Żukowski et al., 1993) was proposed using SPDC as the initial entanglement source. They nevertheless suffer from the same inconvenience as the linear optics set-ups: regardless of being able to excite the non-linearity at relatively high rates, the probabilistic nature of the SPDC sources fundamentally limits its application to quantum information protocols. Therefore the study and development of alternative deterministic entanglement sources that can work on demand is of much relevance.

In this thesis we have thus focused on the later analysis. In particular, we already mentioned that QDs can be excited in a way such that two photons are emitted by means of the biexciton cascade. This pair of photons is in fact entangled in the polarisation degree of freedom of the emitted photons and has been widely investigated as an on-demand entanglement source (Benson et al., 2000; Akopian et al., 2006; Liu et al., 2019; Huber et al., 2018). In **Chapter** 3 we have studied the implementation of a biexciton cascade in a nanophotonic chiral waveguide, experimentally realised by Østfeldt et al. (2022). The chirality of the waveguide translates the polarisation entanglement from the biexciton cascade into a path-entangled state and thus allows for the integration of these entanglement sources in photonic circuits (that typically only support a single polarisation mode).

II. A safe quantum network

The next building block that we focus on is the distribution of the quantum information, similarly to how the classical internet connects our laptops and smartphones nowadays. This network must be able to connect the qubits generated by means of the sources described in the previous subsection with the corresponding receivers, that we will call nodes of the network (see Fig. 2). The nodes can consist of quantum computers, storage stations, or simply the intended recipients of the information, besides further sources. Note that the development of a mature quantum internet is thus not subject to having a universal quantum computer. In fact, a specific number of qubits is not required to show quantum advantage in a quantum network (Wehner et al., 2018).

Since photonic qubits barely interact with their environment and are the fastest in transmission, they are the obvious choice for establishing a network over long distances. Free-space transmission can be implemented through a satellite network (Yin et al., 2020) or free-space links on ground (Ursin et al., 2007), whose main advantage is that the predominant losses occur only at the lowers sections of the atmosphere. This allows for loss-free, long-distance transmission at the height where satellites typically operate. Moreover, fiber transmission is already widely implemented around the globe. It would thus greatly simplify the build-up of the quantum internet to make use of this technology. In fact, there are already many research efforts into generating photonic qubits at telecommunication wavelength (900-950 nm wavelength range) in order to be able to make use of such installations (Da Lio et al., 2022).

With the transmission of qubits through optical fibers follows many challenges that their classical counterparts do not suffer from. Losses in optical fibers scale exponentially with the length of the fiber, having a typical attenuation coefficient of the order of 1-5 dB/km (Fosco-Connect, 2023). This already makes a transmission where the source and the node are separated only by 10 km succeed with 10% probability, which thus makes long distance communication almost impossible due to the low available rates. For classical communication, this issue is soled by means of repeaters that amplify the signal every certain number of kilometers. However, one of the advantages of qubits is that there is no way of systematically making a copy of an arbitrary state (Wootters et al., 1982). As much as this intrinsic consequence of quantum mechanics is a clear asset of quantum communications in terms of safety, it makes the direct implementation of classical repeaters useless. Therefore developing a quantum network entails designing *quantum repeaters* (Sangouard et al., 2011; Ruihong et al., 2019; Borregaard et al., 2020), that take advantage of different entanglement distribution schemes to effectively increase the transmission distance by performing teleportation (Bennett et al., 1993) of the quantum state[5].

[5]Many of the quantum repeater protocols require the use of quantum memories for optimal performance (Andersen, 2019). The storage of quantum information and its challenges will be introduced in the last section of the Introduction.

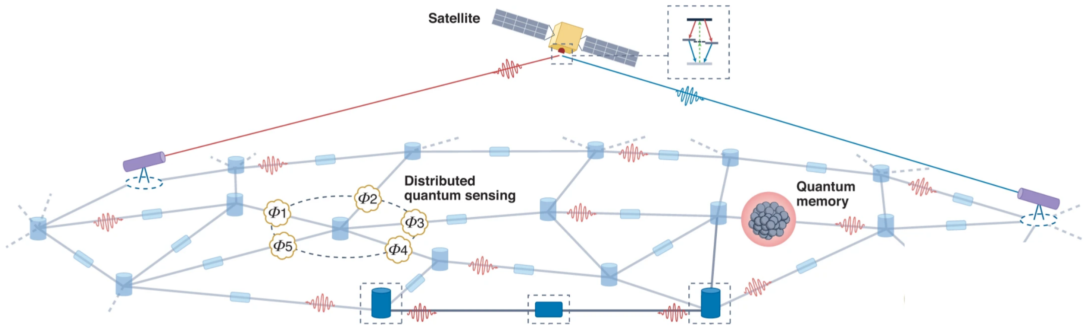


Figure 2: A possible scheme of the quantum internet implementation, with both ground- and satellite photonic links connecting the different nodes, which include quantum memories, repeater stations and quantum computing processors. Adapted from Lu et al. (2021).

The following natural question to ask ourselves is how to make sure that the level of safety of any quantum network is sufficient for today's communications, and its performance in comparison to the security of the current cryptography protocols. We introduce this discussion in the following subsection.

Quantum cryptography

The promise of a universal quantum computer in the near future is an exciting perspective for the progress of numerous fields thanks to its immense computational power compared to classical computers for certain computational tasks. Nevertheless, our current cybersecurity is based on RSA (Rivest et al., 1978) public key protocols. The security of these protocols is based on the computational complexity of the problem needed to solve to break the code. Thus a sufficiently powerful computer can in principle dismantle the task and expose the encrypted information. These types of protocols are thus only *computationally secure*: while solving this problem would take a classical computer an amount of time that exceeds the average human lifespan, a quantum computer could solve it orders of magnitude faster, thanks to its quantum advantage. Therefore, we want to develop a security protocol that, regardless of the computational power of the eavesdropper, can remain secure under a minimal number of assumptions. Such protocols are known as *information-theoretically secure* (Renner et al., 2022). We could thus turn the apparent vulnerable position of our current cybersecurity around by using the same quantum features that empower quantum computers, to develop information-theoretically secure cryptographic schemes.

It can be proven that if a secret string of truly random bits is shared between Alice and Bob[6], they can freely encrypt the information they wish to share in an

[6] Alice and Bob are the usual characters that represent the roles of emitter and receiver in the cryptography jargon. Later we will also need a third person involved in the communication, which is usually called Charlie. Eve is usually the malicious eavesdropper.

information-theoretically secure way (Shannon, 1949). The string of random bits is known as the *secret key* and both Alice and Bob need to be in possession of it *before* any sensitive information is publicly announced between them. The key can only be used once and must be at least as long as the message to be transmitted between Alice and Bob. This technique is known as One Time Pad (OTP) and was already invented by an American banker named Frank Miller in 1882 (Bellovin, 2011). The remaining challenge is to ensure that Alice and Bob can share as many secret keys as needed, and always prior to their communication regardless of their spatial separation. This non-trivial transmission of the key is known as key distribution. Moreover, one can take advantage of quantum mechanics and design a *quantum key distribution* (QKD) version that executes the task in a more secure way than any other classical approach[7].

In the first place, the aforementioned no-cloning theorem (Wootters et al., 1982) prevents any potential eavesdropper from making a direct copy of a qubit transmitted from Alice to Bob. This theorem, however, does not impede Eve from stealing the qubit, measure its state, and resend it to Bob. Luckily her actions on the qubit are noticeable by Bob with a certain probability, since we know from quantum mechanics that performing a measurement over a state essentially perturbs it. The first QKD protocol BB84 (Bennett et al., 1984), and its equivalent version with entanglement distribution E91 (Ekert, 1991), make use of these two quantum characteristics of the qubit to safely transmit the secret key between Alice and Bob. These two protocols, as well as other similar QKD protocols (for state-of-the-art experimental implementations, see for example Yuan et al. (2018) and Boaron et al. (2018) for decoy-state QKD and Wang et al. (2022) for twin field QKD), take nevertheless several assumptions that need to hold in order to ensure security. In particular, regarding the level of trust in the devices utilized in the process. In the following subsection we will introduce a different type of quantum cryptography that relaxes this latter assumption.

Device-Independent Quantum Key Distribution

We have so far qualitatively described how quantum mechanics provides the tools to improve the security of long-distance communications. In particular, QKD protocols like BB84 or E91 can detect the actions of Eve up to a certain error as long as the following assumptions are satisfied (Pironio et al., 2009):

- Alice's and Bob's laboratories are shielded such that no information can leak outside of them. This further means that the classical memories where they store the un-encrypted messages are secure.

[7] Whether a trusted common friend travelling between their locations or a very professional courier company could be strong classical candidates to distribute the secret key will not be discussed. Proving the level of trust in a person or company quantitatively is out of our scope if ever possible, not to speak of the low-rate and high-emissions derived from the related transportation of the secret keys.

- They possess a true random number generator that they trust to generate the random bits needed for basis choice and the generation of the secret key.
- They can communicate via an authenticated classical channel, that is, a channel whose content can be publicly accessed but not manipulated.
- Quantum mechanics is correct.
- Alice and Bob must have certain knowledge about and trust in their quantum devices, which are inaccessible to Eve.

The last assumption is, however, rather hard to fulfill. In an ideal not very far future, Alice and Bob could acquire a couple of boxes from a telecommunications company that promises to perform QKD for them. They would only have to carry out a specified protocol and press certain buttons on the boxes they just bought. However, how can they be certain that these boxes work as they should? Can they ensure that no error occurred during its manufacture that compromises the security of their communication? And what is even worse, Eve could even be the owner of the communications company and mess deliberately with the devices with the worst of the intentions.

Fortunately, one can take a step further to be able to skip the last assumption. *Device-Independent Quantum Key Distribution* (DIQKD) protocols do not rely on trusting the quantum devices thanks to taking advantage of non-local quantum correlations. Consider a situation where the internal functioning of Alice's and Bob's measurement boxes is unknown to them: Alice (Bob) only provides with a classical input a (b) and the box returns a classical output A (B). Their measured statistics are therefore the probabilities $P(A|a)$ and $P(B|b)$ (and thus the also the joint statistics $P(A,B|a,b)$) of obtaining A and B respectively given the inputs a and b. Furthermore, the boxes can be assumed to be accessible by Eve, as the security of the protocol relies fully on the statistics that Alice and Bob measure from them. In particular, a violation of Bell's inequality (Bell, 1964) is required. If the measured statistics do not violate Bell's inequality, then Alice and Bob know that the shared key's secrecy is compromised and thus disregard it and try again.

But why does a failure in violating Bell's inequality mean that Eve attempted an attack? Bell's inequality, in its more common representation: the CHSH form (Clauser et al., 1969), reads

$$E(a,b) + E(a',b) + E(a,b') - E(a',b') \leq 2\,, \tag{3}$$

where $E(a,b)$ is a correlator that depends on the statistics measured by Alice and Bob as

$$E(a,b) = \sum_{i,j} (-1)^{i\oplus j} P(A_i, B_j|a,b)\,, \tag{4}$$

where $\oplus$ represents the modulo-two sum and the main sum runs over the classical outputs A_i and B_j.

Bell's inequality is derived upon the assumption that the correlations between Alice and Bob are both realist and local, which implies that Alice's and Bob's measurements are completely independent and unable to influence the other's outcomes (Bell, 1964). In other words, under these conditions the correlations can be expressed as

$$P(AB|ab) = \sum_{\lambda} P(\lambda)P(A|a,\lambda)P(B|b,\lambda)\,, \tag{5}$$

where λ is known as a classical *hidden variable* that correlates Alice's and Bob's statistics. This would compromise the security of the protocol: Eve could have access to this hidden variable and use this knowledge to infer the secret key. One can show, however, that a maximally entangled state can yield up to a violation of $2\sqrt{2}$ (which is also the maximal violation achievable according to Tsirelson's bound (Cirel'son, 1980)). This means that for certain states the correlations between Alice and Bob can not be described as locally deterministic, and therefore such a hidden variable does not exist. Particularly, the violation of the inequality shows the non-local nature of the correlations making it impossible for a third party to predict these statistics beforehand. Violating Bell's inequality is however experimentally very demanding since there are several loopholes to be closed (Shalm et al., 2015; Hensen et al., 2015; Giustina et al., 2015). In **Chapter** 1 we extensively discuss this and analyse the requirements for violating Bell's inequality with quantum-dot single-photon sources (González-Ruiz et al., 2022b), that were introduced in the Section I. of the Introduction.

Although necessary, a violation of Bell's inequality is unfortunately not sufficient for proving the security of a DIQKD protocol. One needs to prove that it is possible to distil a positive key rate, which is not implied by the violation of the inequality per se. At the end of the day, what we need to demonstrate is that the information accessible by Eve is not larger than that shared between Alice and Bob. To this end we start by introducing several important quantities. The uncertainty contained in any probability distribution $P(x)$ can be quantified with the help of its entropy $H(P)$, known as Shannon entropy,

$$H(P) = -\sum_{x} P(x) \log P(x)\,. \tag{6}$$

We can similarly define the equivalent entropy $S(\rho)$ of a quantum state ρ, the von Neumann entropy[8]

$$S(\rho) = -\operatorname{Tr} \rho \log \rho\,. \tag{7}$$

Moreover the conditional entropy shows how conditioning on classical side information decreases uncertainty as

$$H(A|B) = H(AB) - H(B)\,. \tag{8}$$

[8]In our notation, the von Neumann entropy of a state $S(\rho_A)$ would be the quantum "equivalent" of the classical Shannon case $H(A)$.

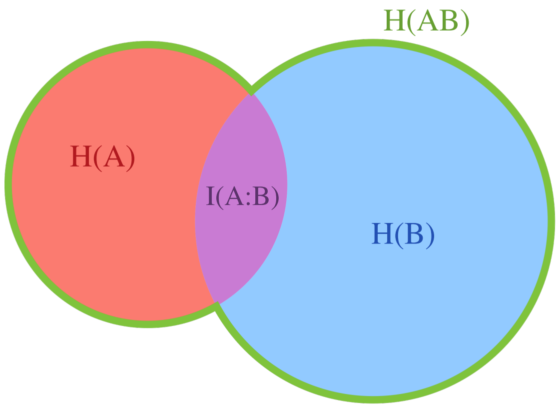


Figure 3: Diagram that shows the relation between Alice's and Bob's entropies ($H(A)$ in red and $H(B)$ in blue, respectively). The entropy of their joint state is given by $H(AB)$ (in green), while their mutual information corresponds to $I(A:B)$ (in purple).

Please note that contrary to the classical conditional entropy, the quantum case can have negative values, for example by means of a maximally entangled state. This is very interesting, since it can be interpreted as "knowing less than nothing" (Gour et al., 2022). We can also define the mutual information between the states ρ_A and ρ_B as

$$I(A:B) = H(A) + H(B) - H(A,B)\,. \tag{9}$$

We can get a better intuition about the mutual information in the sketch depicted in Fig. 3, where we see that it corresponds to the intersection between the entropies of the two systems A and B. The quantum mutual information has nevertheless properties than are essentially different from or nonexistent in its classical counterpart. In particular, the quantum mutual information can be upper bounded by

$$I(A:B) \leq S(\rho_B) - \sum_x P(x)S(\rho_{B,x}) \equiv \chi(A:B)\,, \tag{10}$$

where $\rho_B = \sum_x P(x)\rho_{B,x}$ and the probability distribution depends on the system A (Pironio et al., 2009). This bound $\chi(A:B)$ is called the *Holevo bound* and proves that there is a limit in the accessible information from the system (Nielsen et al., 2010, p. 531). It can also be interpreted as the analogue of mutual information for classical information sent through a quantum channel.

We can now introduce a theorem that allows us to prove the security of a DIQKD protocol. For any state ρ, it holds that

$$r \geq I(A:B) - \chi(B:E)\,, \tag{11}$$

where r is the one-way secret key, $I(A:B)$ is the mutual information shared between Alice and Bob for the specified measurement input, and $\chi(B:E)$ is the Holevo bound on the mutual information shared between Bob and Eve. This theorem is the *Devetak-Winter bound* (Devetak et al., 2005). Intuitively, it shows that a positive key rate can be distilled as long as there is more information shared between Alice and Bob than with the eavesdropper. While $I(A:B)$ is directly obtained from the statistics measured by Alice and Bob, $\chi(B:E)$ is very hard to calculate. It needs to account for all possible strategies from Eve. Proving the security of a DIQKD protocol results in a complex minimisation problem[9] over the joint state between Alice and Bob ρ_{AB}. After the minimisation, one finds the worst case scenario for them, and checks if even in that case a positive key rate is achievable.

DIQKD protocols have been recently implemented experimentally for the first time, by means of trapped Rubidium atoms (Zhang et al., 2022) and ion traps (Nadlinger et al., 2022). In **Chapter** 4 we alternatively analyse the potential of quantum-dot single-photon sources for implementing DIQKD experimentally, using the recent bounding method for $\chi(B:E)$ derived by Brown et al. (2021).

III. Storing the quantum information

Finally we will briefly introduce *quantum memories* and their main challenges for the purpose of storing quantum information. Several of the protocols that we have already mentioned, such most of quantum repeaters or quantum cryptography schemes, require their nodes to be able to keep their qubits unmeasured, but efficiently stored. This is a challenging task, since as we have discussed, decoherence will more or less rapidly erase the quantum features of the stored state.

Since the quantum memories will be located at the nodes of the quantum internet, the physical platform that supports them must mostly focus on having as long coherent times as possible, together with high storage-retrieval efficiency. Some examples of good candidates to be efficient quantum memories are summarized in Simon et al. (2010): solid-state atomic ensembles in rare-earth doped crystals, NV centers in diamond, semiconductor quantum dots, single trapped atoms, room-temperature and cold atomic gases, and optical phonons in bulk diamond. Another system that is an excellent candidate to become a good quantum memory is high-Q optomechanical membranes, since they show coherence times up to ms (Rossi et al., 2018).

All of them, however, face yet another issue: being able to efficiently store the quantum information from the travelling qubit implies being able to "talk" together. This is generally not the case: for example, superconducting qubits typically operate in the microwave wavelength, while quantum-dot single-photons timescale is in the pico-second range, or the aforementioned optomechanical membranes oscillate with MHz frequencies. This imposes a *bandwidth matching* problem. In **Chapter** 5 we propose an experimental implementation to efficiently elongate the pulse length of single-photons in order to match their broad bandwidth with narrower-bandwidth systems, such optomechanical membranes.

[9]These problems are typically computed by means of Semi-Definite Programming (SDP). For more details, see **Chapter** 4.

Structure of the thesis

I. Quantum information sources

- In **Chapter** 1 we present the results published in González-Ruiz et al. (2022a), where we model the experimental imperfections of quantum-dot single-photon sources to analyse their capacity to violate Bell's inequality.
- In **Chapter** 2 we introduce unpublished results soon to be submitted (Bjerlin et al., 2023), where we investigate the relation between the purity of single-photon sources and the indistinguishability of the photons they generate.
- In **Chapter** 3 we show the theoretical analysis presented in González-Ruiz et al. (2023). In this work we present a full theoretical analysis of the entanglement quality of the on-demand path-entangled states generated experimentally by Østfeldt et al. (2022) through a QD biexciton cascade.

II. A safe quantum network

- In **Chapter** 4 we present the submitted results from González-Ruiz et al. (2022b). In this study we take a step further from Chapter 1 by relating the obtainment of non-zero secret-key rates in DIQKD protocols with the experimental imperfections modelled in González-Ruiz et al. (2022a). We thus derive conditions on the single-photon sources that mark the way for near-future implementations of DIQKD protocols.

III. Storing the quantum information

- In **Chapter** 5 we present unpublished work where we introduce a new method to make an efficient bandwidth compression of single photons, in order to be able to store them efficiently in narrow-bandwidth quantum memories.

Chapter 1

Violation of Bell's inequality with quantum-dot single-photon sources

This chapter is based on the work presented in González-Ruiz et al. (2022a)[1]. We investigate the possibility of realizing a loophole-free violation of Bell's inequality using deterministic single-photon sources. We provide a detailed analysis of a scheme to achieve such violations over long distances with immediate extensions to device-independent quantum key distribution. We investigate the effect of key experimental imperfections that are unavoidable in real-world single-photon sources including the finite degree of photon indistinguishability, single-photon purity, and the overall source efficiency. We benchmark the performance requirements to state-of-the-art deterministic single-photon sources based on quantum dots in photonic nanostructures and find that experimental realizations appear to be within reach. We also evaluate the requirements for a post-selected version of the protocol, which relaxes the demanding requirements with respect to the source efficiency.

1.1 Introduction

Violation of Bell's inequality is of fundamental significance for our understanding of nature and has been the subject of a broad experimental endeavour for the last few decades. A complete violation is highly challenging due to the presence of the locality and detection loopholes (Larsson, 2014), which must be closed simultaneously to realize loophole-free experiments (Giustina et al., 2015; Shalm et al., 2015; Hensen et al., 2015). While the locality loophole only requires measurement stations to be sufficiently separated, overcoming the detection loophole demands high transmission efficiencies (Pironio et al., 2009), which is particularly challenging at the

[1]The Ph.D. student was involved in the discussions that shaped the project, discussing together with the supervisor which experimental errors should be included in the study as well as the analysis of the decoherence mechanisms of the single-photon sources. She performed all the calculations and simulations with the supervision of AS. Finally, she wrote the main text and appendices and contributed to the iteration of corrections together with the other co-authors.

large distances required to close the locality loophole. In addition to its fundamental significance, closing the loopholes enables important technological applications. In particular, a detector-loophole-free violation of Bell's inequality is required for device-independent quantum key distribution (DIQKD) (Pironio et al., 2009), which allows ultimately secure communication protected even against hacking attempts on the applied hardware. Although these applications do not necessarily need to close the locality loophole, they impose similar demands since cryptography is based on the communicating parties to be far apart.

Recently three different experiments have successfully closed both loopholes simultaneously. On one side, Bell violation has been achieved based on a heralding scheme with NV centers (Hensen et al., 2015), but the operation of these systems is rather complicated and typically slow leading, e.g., to limited key rates for DIQKD. Faster operations have been achieved in purely photonic systems by exploiting efficient superconducting detectors, but at the cost of only working over short distances (< 200 m) (Giustina et al., 2015; Shalm et al., 2015).

A solution to overcome these problems has been proposed in Kołodyński et al. (2020) based on a photonic approach using deterministic single-photon sources. This method exploits heralding measurements at a central station and is thus applicable to long distances with limited transmission probability. If the photons are transmitted through vacuum this could allow the implementation of loophole-free violation of Bell's inequality. For photons transmitted through optical fibers on the hand, the slower propagation speed in the fibers potentially open the locality loophole (discussed in detail below). Nevertheless the proposal still enables closing the detector loophole over long distances and thus the application of the scheme for DIQKD. The scheme could also be implemented with spontaneous parametric down conversion (SPDC) sources, but this was found to have a less favorable scaling with the transmission efficiency (Kołodyński et al., 2020). For instance it achieves lowers a key rate in DIQKD and this makes an implementation with on-demand single-photon sources more attractive. Real single photons, however, have a number of imperfections which could potentially prevent the violation of Bell's inequality. The influence of these imperfections thus needs to be carefully assessed to determine the applicability of existing single-photon sources.

In this article we theoretically investigate the performance of real single-photon sources for the (detector-)loophole-free Bell test of Kołodyński et al. (2020) taking into account the quality of the single-photon sources and the efficiency of the local stations. We focus on InGaAs quantum dots embedded in a photonic-crystal waveguide as single-photon sources. These have recently shown near ideal performance, generating on-demand single photons with up to a 99.4% purity and 96% indistinguishability (Uppu et al., 2020; Tomm et al., 2021). The results derived here [2] are also applicable to other types of single-photons sources. We investigate the generic imperfections and analyse the relation between the achievable violation of Bell's

[2] The codes used in this study are available at the University of Copenhagen public repository ERDA. DOI: https://doi.org/10.17894/ucph.00388c73-1c04-4005-9138-69fbcd0ebe7a

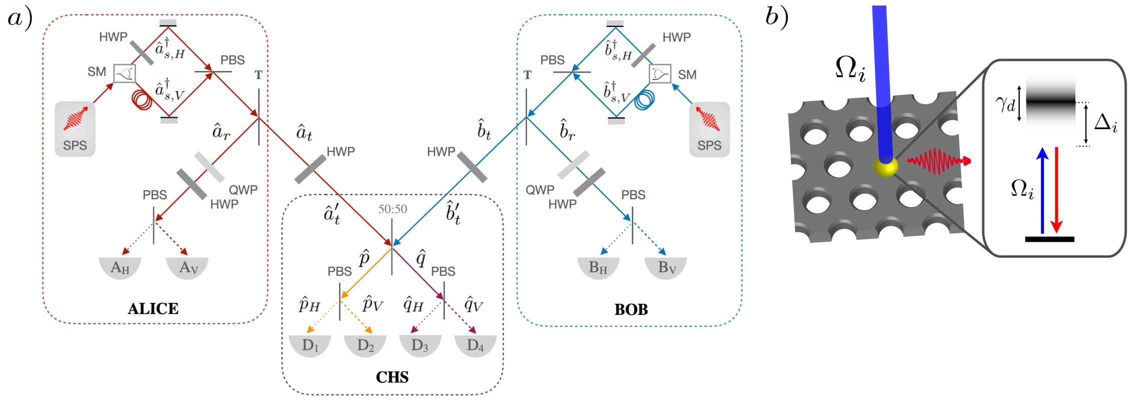


Figure 1.1: *a)* Set-up proposed in Kołodyński et al. (2020), consisting of two local stations (Alice and Bob) and a central heralding station (CHS). The different optical components involved are indicated: beam splitters with transmittances T (at Alice and Bob's stations) and 50% (at the CHS); half and quarter-waveplates (HWP and QWP), switchable mirrors (SM), polarizing beam splitters (PBS) and single-photon sources (SPS). The photodetectors are labeled as D_1, D_2, D_3, and D_4 at the CHS and A_H (B_H) and A_V (B_V) for Alice's (Bob's) detectors, with the sub index indicating the polarization of the corresponding incoming photons. The operators that model the creation of photons at each section of the set-up are indicated as well. *b)* Example of quantum-dot single-photon source and its energy level schemes. The light-matter interaction between a quantum-dot and a waveguide mode is enhanced by the nanostructure realizing a deterministic single-photon source. The quantum dot is driven by a resonant excitation pulse (Ω_i) and subsequently emits a single photon into the waveguide by spontaneous emission. Insert: The optical transitions are subject to two different types of decoherence: 1) rapidly fluctuating phonon interactions induce pure dephasing with a rate γ_d and 2) slow drifts of the levels induce a slowly varying detuning Δ_i.

inequality and the indistinguishability of the generated photons through the Hong-Ou-Mandel (HOM) visibility, their second-order correlation function ($g^{(2)}$) and the single-photon source efficiency. We hope that the analysis will motivate experimental demonstrations of long-distance photonics based (detector-)loophole-free Bell inequality violations in the near future.

1.2 Ideal implementation

We investigate the scheme originally put forward in Kołodyński et al. (2020). It is based on a heralding scheme in which two parties, Alice and Bob, each generate a pair of single photons with orthogonal polarization (see Fig. 1.1). Here we will consider an implementation based on having only a single on-demand single-photon source at each station. As we will show below an implementation based on subsequent emissions from the same source is highly advantageous since several imperfections associated with slow drifts in the sources naturally cancel out.

The single-photon sources each emit a pair of photons with vertical polarization but with one of them delayed in time with respect to the other. The photons are sent to different optical paths by means of a switchable mirror. The early photon is sent through the longest arm, while the late photon is sent to the short arm and is rotated to horizontal polarisation with a half-wave plate. The early and late photons arrive simultaneously at a polarizing beam-splitter (PBS), which merges the two inputs generating a state described by

$$\hat{a}^{\dagger}_{s,H}\hat{a}^{\dagger}_{s,V}\left|\emptyset\right\rangle_{A} = \left|1_H\right\rangle\left|1_V\right\rangle_{A}, \quad \hat{b}^{\dagger}_{s,H}\hat{b}^{\dagger}_{s,V}\left|\emptyset\right\rangle_{B} = \left|1_H\right\rangle\left|1_V\right\rangle_{B}, \tag{1.1}$$

where $\hat{a}^{\dagger}_{s}$ ($\hat{b}^{\dagger}_{s}$) denotes the photon creation operator acting on the vacuum state $\left|\emptyset\right\rangle$ either at Alice's (A) or Bob's (B) station, with the second index denoting horizontal (H) or vertical (V) polarization.

After the PBS, the photon pair is sent towards a beam-splitter of transmittance T. The reflected field is then sent to a detection set-up, whereas the transmitted field is sent towards a central heralding station (CHS) placed between Alice and Bob. At the CHS the photons pass through additional optical components until they are finally detected by four single photon detectors D_l with $l = 1, ..4$. As we will show later, entanglement will be generated if the photons detected at the CHS have orthogonal polarization. This restricts the possible accepted detection patterns to clicks on pairs of detectors D_1D_2, D_3D_4, D_1D_4 and D_2D_3 (see Fig. 1.1).

Ideally, two photons (one from each side) are transmitted to the CHS while the other photons remain in the station where they were generated. At the CHS, Bell state measurements on the received photons are performed (Kwiat et al., 1998) thereby creating a polarization entangled state between the photons that remained in the local stations. Importantly, the protocol is still applicable even for a very low transmission probability to the CHS, since photon loss only reduces the heralding rate but not the performance of the protocol. Finally, Alice and Bob measure their respective qubits by means of a pair of half-wave and quarter-wave plates (HWP and QWP) and a pair of photodetectors.

The basic operational principle of the set up is that of the Hong-Ou-Mandel (HOM) effect (Hong et al., 1987). In each station, beam splitters of transmittance T transmit single photons from Alice and Bob to the CHS. Conditioning on two clicks at the CHS means that at least two photons were transmitted, and by choosing a low transmittance $T \ll 1$ we ensure that there is a negligible probability of transmitting more than two. In this case there will thus be two photons at Alice and Bob's stations for the final Bell's test with a very high probability if $T \ll 1$. The two photons at the CHS photons could, however, be from the same station, such that either Alice or Bob will have two photons while the other would have none. To exclude this possibility a HWP is inserted in each of the arms leading to the CHS. This HWP rotates each of the polarizations by 45 degrees. Seen in the horizontal-vertical basis the HWP essentially acts as a beam-splitter transformation between the two polarization states described by

$$\hat{a}^{\dagger}_{H} \to \frac{1}{\sqrt{2}}\left(\hat{a}^{\dagger}_{H} + \hat{a}^{\dagger}_{V}\right), \quad \hat{a}^{\dagger}_{V} \to \frac{1}{\sqrt{2}}\left(\hat{a}^{\dagger}_{H} - \hat{a}^{\dagger}_{V}\right). \tag{1.2}$$

Thereby it acts as a beam splitter in a HOM-like setup such that two photons in the same arm will bunch and never end up with opposite polarization when measured in the horizontal-vertical basis. Conditioning on photons with different polarization will thus ensure that the detected photons came from different stations and that there is always a photon at both Alice and Bob's stations.

If the two photons transmitted to the heralding station have the same polarization they will bunch at the 50:50 central beam splitter due to their indistinguishability, leading to the possible detector combinations D_1D_2 and D_3D_4. These patterns do not, however, provide any information about the initial polarization of the photons before the HWP except that they were identical. Thus, the state of the pair that Alice and Bob will share in this case is the Bell state $|\phi^-\rangle = \frac{1}{\sqrt{2}}\left(\hat{a}_H^\dagger\hat{b}_H^\dagger - \hat{a}_V^\dagger\hat{b}_V^\dagger\right)|\emptyset\rangle$ (with the minus sign coming from a more detailed analysis of the protocol).

On the other hand, if the pair of photons arriving at the CHS has opposite polarizations, they are distinguishable and therefore will not show the HOM bunching effect at the beam splitter. If they are transmitted to the same port of the beam splitter they will click on the same detector since the PBS acts as a HOM setup for the photons encoded in diagonal polarizations by the HWPs and will be discarded. On the contrary, if they are transmitted to different PBS, the combinations D_1D_4 and D_2D_3 can occur and since their polarizations were initially different, the state that Alice and Bob share must be proportional to $|\psi^-\rangle = \frac{1}{\sqrt{2}}\left(\hat{a}_H^\dagger\hat{b}_V^\dagger - \hat{a}_V^\dagger\hat{b}_H^\dagger\right)|\emptyset\rangle$ (again the minus sign is found from a more detailed analysis).

From the above analysis we thus find that recording clicks in detectors with opposite polarizations implies that there will be a photon at each of Alice and Bob's stations prepared in an entangled state conditioned on the outcome at the CHS. Subsequent measurements in different bases implemented by rotating the polarization with the HWPs and QWPs at the local stations can then be used to demonstrate the violation of Bell's inequality. The combinations that generate entanglement (D_1D_2, D_3D_4, D_1D_4 and D_2D_3) represent 50% of the total number of detection events. This is in accordance with the fact that any linear-optical circuit that performs Bell-state measurement can only generate distinguishable entangled states with at most 50% probability (Calsamiglia et al., 2001). In particular, in this work we analyse the state heralded by the detection patterns D_1D_4 and D_2D_3, which is $|\psi^-\rangle$.

From the above idealized description it is clear that the protocol relies heavily on high-quality single-photon sources. In practice, real sources will always have small multi-photon components and non-perfect indistinguishability. In addition, optical systems are prone to losses. To assess the performance of the protocol for real sources we thus need to evaluate the effect of these imperfections.

1.3 Model for real sources

The ultimate purpose of this work is to analyse the influence that the quality of a realistic single-photon source can have on the success of the protocol. In this section we present the main parameters that describe the source. We will account both

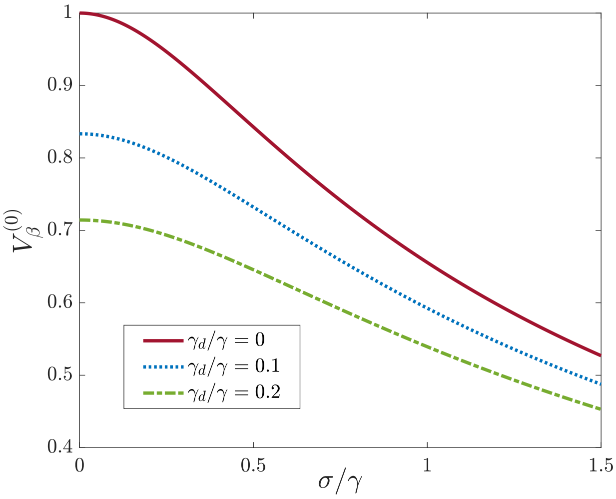


Figure 1.2: Degree of indistinguishability of photons from different sources, i.e. the HOM visibility $V_\beta^{(0)}$. The indistinguishability depends on the width σ of the probability distribution for the frequency fluctuations Δ as well as the rate of pure dephasing γ_d relative to the spontaneous emission rate γ.

for the loss of indistinguishability of photons due to decoherence processes and the purity of the source, as well as the efficiency of the set-up.

1.3.1 Dephasing

The single-photon source i emits a photon in a state $\hat{a}_i^\dagger |\emptyset\rangle$. Here the single mode operators $\hat{a}_i$ fulfill the single mode commutation relation $[\hat{a}_i, \hat{a}_j^\dagger] = \delta_{ij}$ and are defined by

$$\hat{a}_i = \int_{-\infty}^{\infty} f_i(t)\hat{a}_i(t)dt\,, \tag{1.3}$$

where $\hat{a}_i(t)$ is a photon annihilation operator for a photon at time t fulfilling the continuous time commutation relations $\left[\hat{a}(t), \hat{a}^\dagger(t')\right] = \delta(t-t')$, $[\hat{a}(t), \hat{a}(t')] = \left[\hat{a}^\dagger(t), \hat{a}^\dagger(t')\right] = 0$. We have here introduced the function $f_i(t)$, with $i \in \{1, 2, 3, 4\}$, (different for every source in which the photons are generated) which describes the shape of each photons wavepacket. $f_i(t)$ convolutes each photon's creation operator differently in time, according to the properties of the emitter. Ideally $f_i(t)$ will be the same for all sources, resulting in fully indistinguishable photons. Variations between emitters and temporal fluctuations, however, imply that they may vary between different emitters and between different experimental runs. These functions thus encode the relevant photon coherences.

The functions $f_i(t)$ satisfy the normalization $\int_{-\infty}^{\infty} |f_i(t)|^2 dt = 1$ and their overlap defines the degree of *indistinguishability* of the photons, that we define as α_{ij} or β_{ij} depending on whether the pair of photons was produced at the same or different stations:

$$\left\langle \hat{a}_i(t)\hat{a}_j^\dagger(t')\right\rangle = \int_{-\infty}^{\infty} f_i^*(t) f_j(t) dt \equiv \begin{cases} \alpha_{ij}, & \text{if} \quad ij = 12, 34 \\ \beta_{ij}, & \text{if} \quad ij = 13, 14, 23, 24 \end{cases} . \tag{1.4}$$

This distinction between photons generated at the same or opposite stations is important, since their degree of indistinguishability is expected to be different ($\alpha_{ij} > \beta_{ij}$) because sources at the same station are likely easier to be identical. We can relate α_{ij} or β_{ij} to the raw HOM visibility $V_{\alpha,\beta}^{(0)}$ by calculating the probability of detecting coincidence counts after a 50:50 beam splitter, obtaining $P_{cc} = \frac{1}{2}\left(1 - |\alpha_{ij}|^2\right)$ (or β_{ij}, if photons were generated at different stations). Given that the maximum probability of coincidence counts that can be achieved is $P_{max} = 1/2$, we obtain the relation between visibility and mode overlap (Brańczyk, 2017):

$$V_\alpha^{(0)} = 1 - \frac{P_{cc}}{P_{max}} = \overline{|\alpha_{ij}|^2}\,, \tag{1.5}$$

where we have defined $\overline{X}$ to be the average of the quantity X over all experimental runs due to the variability of $f_i(t)$.

The convoluting functions $f_i(t)$ contain the decoherence processes of the quantum dot that decrease the indistinguishability of the emitted photons. Generally decoherence arises due to a number of different mechanisms acting on different time scales. We divide these processes into two categories: slow and fast processes relative to the decay rate of the emitter. For quantum dot sources the fast process originates from phonon dephasing, whereas intrinsic charge or nuclear spin noise as well as drift in the experimental setup will contribute to the slow detuning processes (Uppu et al., 2021b). We assume that the two photons generated at each station are obtained by multiplexing photons emitted from the same quantum dot (Hummel et al., 2019), i.e. photons from the same stations are insensitive to slow processes, which will have the same influence on two consecutive photons, but will be affected by fast processes which change the mode function $f_i(t)$ between the two photons. On the contrary, photons emitted from different stations will also be affected by slow drift depending on the degree to which these can be stabilized between the distant emitters.

The fast processes are modeled as white noise with a pure dephasing rate γ_d corresponding to the typical model used to describe phonon dephasing (Tighineanu et al., 2018; Muljarov et al., 2004). In Appendix A.1 we show that this leads to a visibility

$$V_\alpha^{(0)} = \overline{|\alpha_{ij}|^2} = \frac{\gamma}{\gamma + 2\gamma_d}\,, \tag{1.6}$$

where γ is the spontaneous decay rate of the quantum dot.

The crossed visibility, $V_\beta^{(0)}$, is also affected by the slow dephasing processes that creates an energy difference Δ_{ij} in the frequency splitting between quantum dots. This difference is assumed to follow a Gaussian distribution with a width σ when averaging over the experimental runs. Evaluating the visibility for detuned emitters and performing the average we obtain the averaged visibility

$$V_\beta^{(0)} = \overline{|\beta_{ij}|^2} = \sqrt{\frac{\pi}{2}} \frac{\gamma}{\sigma} e^{\frac{(\gamma+2\gamma_d)^2}{2\sigma^2}} \operatorname{erfc}\left(\frac{\gamma + 2\gamma_d}{\sqrt{2}\sigma}\right) . \tag{1.7}$$

A similar result was obtained in Kambs et al. (2018).

In Fig. 1.2 we show the relation between visibility and width of the distribution for various dephasing rates. The relations derived in Eqs. (4.4) and (1.7) between the intrinsic parameters of the quantum dot and the indistinguishability of the emitted photons can be used to calibrate the width σ to the measured HOM visibility through Eq. (1.5). For the remaining of this article all plots will thus be shown as a function of the experimentally accessible visibilities $V_\alpha^{(0)}$ and $V_\beta^{(0)}$ rather than γ_d and σ. We note however, that expressing it in terms of visibilities is dependent on the specific model we have assumed for the noise. Below we shall also need higher order moments e.g. $\langle \alpha_{ij}\beta_{ik}\beta_{jk}\rangle$. Such higher order correlations cannot be directly related to the visibility, which only depends on second order moments. Any relation between higher order terms and the HOM visibility will thus always be model dependent.

1.3.2 Optical loss

Although the heralding scheme ensures that the outcome of the protocol is not affected by the transmission efficiency between stations η_t, we must account for losses occurring locally since such losses potentially open the detection loophole. We define $\eta_{1,i}$ as the probability to reach the first beam splitter, and $\eta_{2,i}$ as the probability for the reflected photons to be detected (including detection efficiency) as sketched in Fig. 1.3. The additional index $i = 1, 2, 3, 4$ specifies the source that generated the photon. This distinction between sources is for instance relevant in demultiplexing schemes, which can have different efficiencies in the different channels of transmission (Hummel et al., 2019). Including the losses at the beam splitter, the local efficiency $\eta_{l,i}$ is therefore given by $\eta_{l,i} \equiv \eta_{1,i}\eta_{2,i}(1 - T)$.

Experimentally, the coupling of light from quantum dots to photonic nanostructures has been proven to reach up to 98% (Arcari et al., 2014). As it will be quantified below, the main challenge will be to couple the photons from the nanostructure and to a detector with near-unity efficiency. With a demultiplexed single-photon source this would require highly-efficient coupling of the photon source to a fiber combined with efficient switching and detection. A significant step towards this demanding goal was the recent demonstration of a fiber-coupled device with 57% overall efficiency (Tomm et al., 2021). Another implementation would require operating two quantum dots per station that are mutually interfered. In such a configuration the two sources and detectors could potentially be integrated on a single chip, which likely would be the most efficient approach. A bottleneck for this implementation would be the need to make two quantum-dot sources indistinguishable, but encouragingly 93% HOM visibility was recently reported between two remote quantum

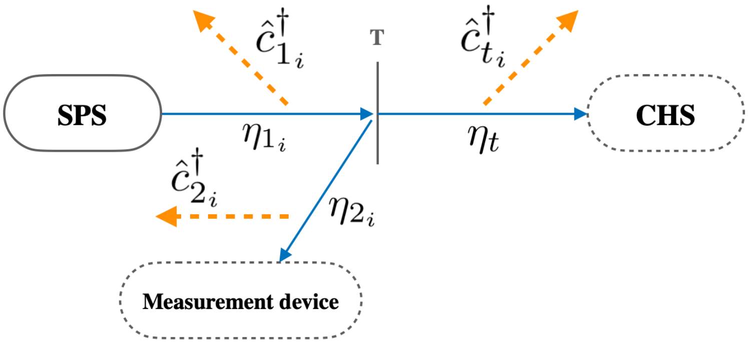


Figure 1.3: Sketch of the efficiencies η_i and definitions of the creation operators of the lost photons $\hat{c}^\dagger$.

dots (Zhai et al., 2021).

1.3.3 Purity

Finally, we consider that the single-photon sources might in fact emit two or more photons at once with a certain probability. This generates the state $\hat{\rho} = P_0\hat{\rho}_0 + P_1\hat{\rho}_1 + P_2\hat{\rho}_2 + \mathcal{O}(P_3)$, where $\hat{\rho}_k$ is the density matrix representing the state of the k-th photon component. The multi-photon component would originate in an experiment either from imperfect suppression of the optical pulses used to pump the quantum dot or from multi-photon emission due to the finite duration of the excitation pulse.

We furthermore assume that the probability for the quantum dot not to emit a photon is negligible $P_0 \simeq 0$, so that $P_1 + P_2 = 1$. This limit is valid as long as the lack of creation of photons by the quantum dot is included in the efficiency parameters $\eta_{1,i}$.

The effect of multi-photon generation can be measured via the second order correlation function $g^{(2)}$

$$g^{(2)} = \frac{\left\langle \iint d\tau_1 d\tau_2 \hat{a}^\dagger(\tau_1)\hat{a}^\dagger(\tau_2)\hat{a}(\tau_2)\hat{a}(\tau_1)\right\rangle}{\langle \int d\tau_1 \hat{a}^\dagger(\tau_1)\hat{a}(\tau_1)\rangle \langle \int d\tau_2 \hat{a}^\dagger(\tau_2)\hat{a}(\tau_2)\rangle}\,, \tag{1.8}$$

which, for the multi-photon state $\hat{\rho}$ yields

$$g^{(2)} = \frac{2P_2}{(P_1 + 2P_2)^2} \simeq \frac{2P_2}{P_1^2}\,, \tag{1.9}$$

to first order in P_2. Throughout this paper we consider the limit $g^{(2)} \ll 1$ such that the probability that more than one photon is emitted by more than one of the sources is negligible. This means that all results derived here should be considered lowest order expansion in $g^{(2)}$ and are only applicable in the limit $g^{(2)} \lesssim 0.1$. Moreover, the second-emitted photon is modelled to be completely distinguishable from the other four photons. The purity of the source will affect the measured HOM visibility $V_{\alpha,\beta}$

with a small contribution proportional to $g^{(2)}$:

$$V_{\alpha,\beta} = V^{(0)}_{\alpha,\beta} - \kappa g^{(2)}\,, \tag{1.10}$$

where in general $1 < \kappa < 3$, depending on the distinguishability of the 1 and 2-photon components. For the model considered here, $\kappa = 2$ where the additional photon is assumed to be fully distinguishable. (Ollivier et al., 2021; Bjerlin et al., 2023). In the following, when plotting quantities as a function of $V^{(0)}_{\alpha,\beta}$ we refer to the value which would be obtained in the absence of any two photon contribution. Hence $V^{(0)}_{\alpha,\beta}$ will be higher than the values measured experimentally.

1.4 Analysis

Having defined the model used to describe the imperfections, we now turn to the analysis of the performance of the protocol. We do this by analyzing how each of the field operators transform in the Heisenberg picture under the linear optics setup shown in Fig. 1.1 when the losses in Fig. 1.3 are taken into account. After this transformation we then evaluate all expressions using the model for the real single-photon sources.

After being generated, the two pairs of photons with orthogonal polarization will encounter a beam splitter with transmittance T, that transforms the creation operators according to

$$\hat{a}^\dagger_{s,\varsigma} = i\sqrt{1-T}\hat{a}^\dagger_\varsigma + \sqrt{T}\hat{a}^\dagger_{t,\varsigma}\,, \tag{1.11}$$

and similarly for Bob's photons, where $\hat{a}^\dagger_\varsigma$ represents a reflected photon at the first beam splitter with polarization $\varsigma \in \{H, V\}$ and $\hat{a}^\dagger_{t,\varsigma}$ a transmitted one. Next, by fixing the angle $\phi = -\pi/8$ for both HWP, we see that the transmitted photons are transformed as:

$$\hat{a}^\dagger_{s,\varsigma} = i\sqrt{1-T}\hat{a}^\dagger_\varsigma + \sqrt{\frac{\eta_t T}{2}}(\hat{a}'^\dagger_{t,H} \pm \hat{a}'^\dagger_{t,V})\,. \tag{1.12}$$

where we have inserted the probability of successful transmission between Alice and Bob and the CHS, η_t. Since we include losses, this transformation should, in principle, also include creation operators for the lost photons. However, since we consider photon counting (and multi-photon errors are considered separately below), such lost photons do not contribute to the final results and we omit the lost photon terms for brevity. Once the photons reach the heralded station they encounter another beam splitter, this time with 50% transmittance, followed by polarizing beam splitters that direct horizontally (vertically) polarized photons to detectors D_1 and D_3 (D_2 and D_4).

We can now incorporate all the steps into a single transformation of the initial operators $\hat{a}^\dagger_S$ ($\hat{b}^\dagger_S$), obtaining

$$\hat{a}^\dagger_{s,\varsigma,i} \rightarrow \sqrt{\frac{\eta_{1,i}\eta_t T}{2}}\hat{O}^\dagger_i + i\sqrt{\eta_{1,i}\eta_{2,i}(1-T)}\hat{a}^\dagger_{\varsigma,i} + \hat{L}^\dagger_i\,, \tag{1.13}$$

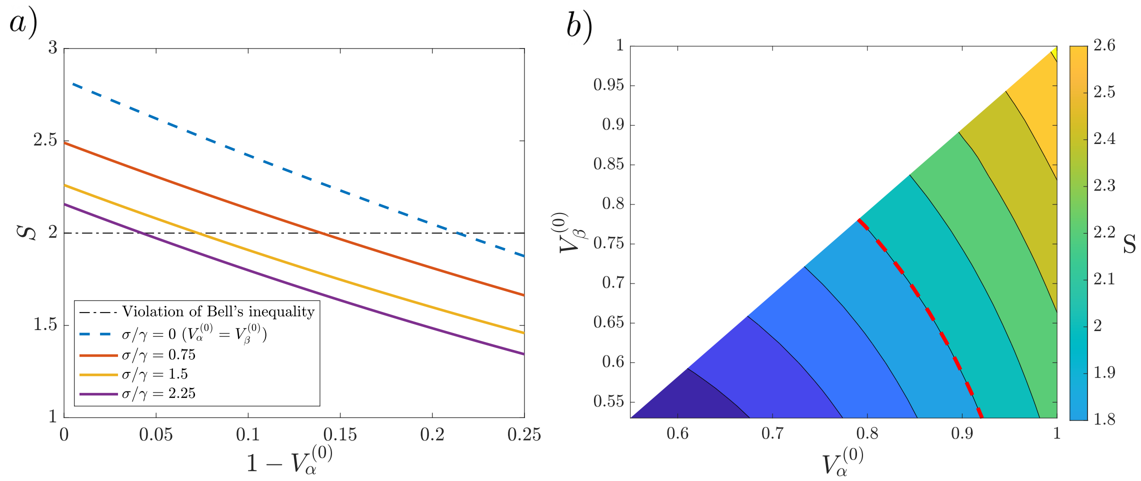


Figure 1.4: *a)* Violation of the CHSH inequality $S \geq 2$, as a function of the HOM visibility of the local sources $V_\alpha^{(0)}$. The curves represent both the case in which photons from Alice and Bob's stations and equally indistinguishable ($V_\alpha^{(0)} = V_\beta^{(0)}$) and when there is inhomogeneous broadening with a width $\sigma \neq 0$ so that $V_\alpha^{(0)} > V_\beta^{(0)}$. The threshold for CHSH violation $S = 2$ corresponds to the visibilities $(V_\alpha^{(0)}, V_\beta^{(0)}) = \{(0.79, 0.79), (0.86, 0.67), (0.93, 0.51), (0.96, 0.40)\}$. *b)* Contour plot of the CHSH value S as a function of the visibilities V_α and V_β. The dashed isoline $S = 2$ delimits the regions with and without violation of Bell's inequality.

and similarly for Bob's operators. We have here defined creation operators for photons at the CHS as

$$\hat{O}^\dagger_{1,2} \equiv \frac{1}{\sqrt{2}} \left(i \left(p^\dagger_{H,1,2} \pm p^\dagger_{V,1,2} \right) + \left(q^\dagger_{H,1,2} \pm q^\dagger_{V,1,2} \right) \right),$$
$$\hat{O}^\dagger_{3,4} \equiv \frac{1}{\sqrt{2}} \left(\left(p^\dagger_{H,3,4} \pm p^\dagger_{V,3,4} \right) + i \left(q^\dagger_{H,3,4} \pm q^\dagger_{V,3,4} \right) \right). \quad (1.14)$$

Eq. (B.7) expresses that a photon can be either successfully transmitted to the CHS ($\hat{O}^\dagger_i$), reflected at the first beam splitter and detected locally ($\hat{a}^\dagger_{\varsigma,i}$) or lost ($\hat{L}^\dagger_i$). The definition of these operators simplify the transformation applied to the initial state and is described in detail in Appendix A.2.

Eq. (B.7) allows us to calculate the density matrix $\hat{\rho}$ shared by Alice and Bob after the heralding by just tracing the CHS and loss operators out from the initial state conditioned on the correct detection patterns:

$$\hat{\rho} = \mathrm{Tr}_{\mathrm{loss},CHS} \left\{ \hat{a}^\dagger_{s,H} \hat{a}^\dagger_{s,V} \hat{b}^\dagger_{s,H} \hat{b}^\dagger_{s,V} \left| \emptyset \right\rangle \left\langle \emptyset \right| \hat{a}_{s,H} \hat{a}_{s,V} \hat{b}_{s,H} \hat{b}_{s,V} \right\}, \quad (1.15)$$

where the partial trace of the CHS is already conditioned to the accepted measurement outcomes $D_1 D_4$ and $D_2 D_3$.

Alice and Bob measure this state by means of two consecutive QWP and HWP, with the total transformation $\hat{U}_{tot}(\theta, \phi) = \hat{U}_{HWP}(\phi) \hat{U}_{QWP}(\theta)$ (Appendix A.2). It transforms the creation operators of the photons into the operators $\hat{A}_H^\dagger$ and $\hat{A}_V^\dagger$ ($\hat{B}_H^\dagger$ and $\hat{B}_V^\dagger$), which represent the creation operators at the corresponding detectors (see Fig. 1.1):

$$\hat{\mathbf{A}} \equiv \begin{pmatrix} \hat{A}_H \\ \hat{A}_V \end{pmatrix} = \hat{U}_{tot}(\theta_A, \phi_A) \begin{pmatrix} \hat{a}_{H,1} \\ \hat{a}_{V,2} \end{pmatrix} \equiv \hat{U}_{tot}(\theta_A, \phi_A)\hat{\mathbf{a}} \tag{1.16}$$

, and similarly with Bob's operators. We further define the measurement operators $\hat{M}_{+,A} \equiv \mathbb{I} - |\emptyset\rangle\langle\emptyset|_{A,H}$ and $\hat{M}_{-,A} \equiv \mathbb{I} - |\emptyset\rangle\langle\emptyset|_{A,V}$, and similarly for Bob. These operators project into the subspace in which any number of clicks occurs at the detectors. We thus assume that the detectors cannot distinguish how many photons arrived but only measure the presence or absence of photons. Events in which there is a wrong number of photons involved are thus also included. We identify a click in the detectors A_H and B_H with an outcome $+$, and A_V and B_V with $-$. We can then calculate the joint probability $P_{x,y}$ that the outcomes $x, y \in \{+, -\}$ are simultaneously measured by Alice and Bob as

$$P_{x,y} = \mathrm{Tr}\left\{\hat{M}_{x,y}\hat{\rho}'\right\}, \tag{1.17}$$

where $\hat{M}_{x,y} = \hat{M}_{x,A} \otimes \hat{M}_{y,B}$ and we have defined:

$$\hat{\rho}' = \hat{U}_{tot}(\theta_A, \theta_B, \phi_A, \phi_B)\hat{\rho}\hat{U}_{tot}^\dagger(\theta_A, \theta_B, \phi_A, \phi_B), \tag{1.18}$$

and $\hat{U}_{tot}(\theta_A, \theta_B, \phi_A, \phi_B) = \hat{U}_{tot}(\theta_A, \phi_A) \otimes \hat{U}_{tot}(\theta_B, \phi_B)$. Note that for convenience the probabilities defined here, include the probability of detecting the photons at the CHS. We therefore need to normalize the probabilities with the success probability when we want to evaluate results conditioned on detections at the CHS. This allows us to calculate the CHSH (Clauser et al., 1969) correlations $C(\mathbf{a}, \mathbf{b}) = \mathbf{ab}$, where $\mathbf{a}$ and $\mathbf{b}$ are two unitary observables that can take the values $\{-1, 1\}$, as a function of the projected probabilities:

$$C(\mathbf{a}, \mathbf{b}) = \frac{P_{+,+} - P_{+,-} - P_{-,+} + P_{-,-}}{P_{success}}, \tag{1.19}$$

where the choice of $\mathbf{a}$ and $\mathbf{b}$ is determined by the HWP and QWP angles θ_A, θ_B, ϕ_A, and ϕ_B. Note that the denominator of Eq. (1.4), $P_{success}$, corresponds to the total success probability for the photons to arrive at the heralding station conditioned on the correct measurement outcomes D_1D_4 and D_2D_3. We can now analyse how the violation of the CHSH inequality

$$S = |C(\mathbf{a}, \mathbf{b}) + C(\mathbf{a}', \mathbf{b}) + C(\mathbf{a}, \mathbf{b}') - C(\mathbf{a}', \mathbf{b}')| \leq 2, \tag{1.20}$$

is affected by all the processes related to real sources described in Section 1.3.

1.4.1 Effect of distinguishability of photons

We start by analysing solely the influence of decoherence of the emitter, ignoring multi-photon generation ($g^{(2)} = 0$) and local losses ($\eta_{l,i} = 1$). Furthermore, we assume for now that apart from the decoherence the protocol behaves ideally: Alice and Bob keep one photon each and send one to the CHS, which is detected in the desired patterns. Physically, this corresponds to post selecting only events where there are always two detected photons at the CHS and one at each station. Applying these conditions to the transformation in Eq. (B.7) and operating on the initial state, we obtain:

$$|\psi\rangle = -\frac{\eta_t T(1-T)}{2}(\hat{O}_2^\dagger \hat{O}_4^\dagger \hat{a}_{H,1}^\dagger \hat{b}_{H,3}^\dagger + \hat{O}_2^\dagger \hat{O}_3^\dagger \hat{a}_{H,1}^\dagger \hat{b}_{V,4}^\dagger + \hat{O}_1^\dagger \hat{O}_4^\dagger \hat{a}_{V,2}^\dagger \hat{b}_{H,3}^\dagger + \hat{O}_1^\dagger \hat{O}_3^\dagger \hat{a}_{V,2}^\dagger \hat{b}_{V,4}^\dagger) |\emptyset\rangle \ . \quad (1.21)$$

We then calculate the partial trace over the the CHS described by the operators $\hat{O}_i^\dagger$. Contrary to the ideal case, the state shared by Alice and Bob after conditioning on the desired detection pattern is no longer a pure state due to the imperfect indistinguishability of the photons. This can be seen from the (unnormalized) density matrix obtained by conditioning on the correct detection patterns $\left\langle \hat{O}_i \hat{O}_j \hat{O}_k^\dagger \hat{O}_l^\dagger \right\rangle_{D1D4,D2D3}$. The full results are given in Appendix A.3. For simplicity we here only reproduce the density matrix in a simpler form assuming $\alpha_{ij} \equiv \alpha$ and $\beta_{ij} \equiv \beta$ for all i, j:

$$\hat{\rho} = \frac{{\eta_t}^2 T^2 (1-T)^2}{4} \begin{pmatrix} 1-|\beta|^2 & 0 & 0 & |\beta|^2-|\alpha|^2 \\ 0 & 1+|\beta|^2 & -\left(|\alpha|^2+|\beta|^2\right) & 0 \\ 0 & -\left(|\alpha|^2+|\beta|^2\right) & 1+|\beta|^2 & 0 \\ |\beta|^2-|\alpha|^2 & 0 & 0 & 1-|\beta|^2 \end{pmatrix}, \quad (1.22)$$

where we have applied the definitions for indistinguishability introduced in Eq. (1.4). The density matrix shown in Eq. (1.22) is written in a basis that is dependent on polarization, as well as the mode functions which may vary from shot to shot of the experiment. This dependence will be traced out once the measurement at the local stations is performed. Note that the state described by Eq. (1.22) is a mixed state in contrast to the indistinguishable limit ($\alpha = \beta = 1$), in which we in fact recover the pure state $|\psi^-\rangle$.

We can now evaluate the results of the measurement with the density matrix $\hat{\rho}$ and calculate the different joint probability contributions by means of Eqs. (1.4) and (1.4). We note, however, that the density matrix in Eq. (1.22) is expressed in terms of photon operators which also contain mode functions that vary in time due to noise. All expectation values will involve a total of 8 mode functions f_i, which we need to average over. Therefore, this results in higher order moments in α_{ij} and β_{ij}, which have to be averaged e.g. giving terms of the form $\overline{\alpha^2\beta^2}$.

We calculate the value of the CHSH Bell parameter S as a function of the HOM visibility $V_\alpha^{(0)}$, that is, the HOM visibility of the sources from the same station (see Fig. 1.4(a)). We study two different limits: first, we consider the limit in which all photons are equally indistinguishable ($\alpha = \beta$). An optimization over the measurement angles is carried out for each value of the visibility in other to maximise S. In this limit a HOM visibility of at least $\approx 79\%$ is needed to violate

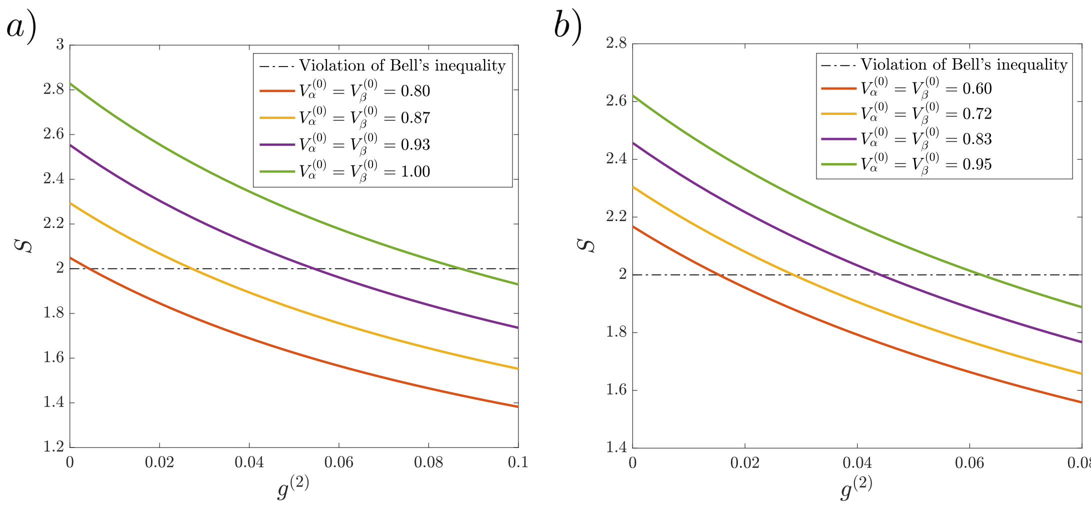


Figure 1.5: Evaluation of CHSH threshold for a postselected protocol and with finite multi-photon contributions. In both figures the CHSH parameter S is shown as a function of the second order correlation function for different values of the HOM visibility, in the limit in which the transmission and local efficiencies are low ($\eta_t = \eta_{2,i} = 0.1$) and for post-selected events. As post-selection is performed, we set $T = 0.5$, which will increase the heralding rate without affecting the performance of the protocol. *a)* The crossed and local HOM visibilities V_α and V_β are identical. *b)* The local HOM visibility is fixed to $V_\alpha = 0.95$ and V_β varies between 0.6 and V_α.

Bell's inequality. We further study the limit in which the cross visibility $V_\beta^{(0)}$ from both stations is lower than the visibility from the same station $V_\alpha^{(0)}$ by varying the inhomogeneous broadening σ. As shown in Fig. 1.4(a), with increasing slow spectral diffusion a higher visibility of the photons from the same stations is required to achieve a Bell violation. In Fig. 1.4(b) we show the size of the violation for all sets of visibilities, keeping in mind that $V_\alpha^{(0)} \geq V_\beta^{(0)}$. Note that if a good local visibility $V_\alpha^{(0)}$ is achieved, the requirement for the crossed visibility $V_\beta^{(0)}$ between stations is rather limited. Remarkably and as an exemplary case, for the experimentally realized value of $V_\alpha^{(0)} = 96\%$ (Uppu et al., 2020) it suffices to reach $V_\beta^{(0)} > 40\%$ to violate Bell's inequality. This is an encouraging requirement that seems well within reach with quantum-dot sources.

1.4.2 Losses and multi-photon errors

When losses and multi-photon errors are included the detection of the correct patterns at the CHS does not guarantee that Alice and Bob share the state predicted by Eq. (1.22). For instance, Alice and Bob might get a positive message from the CHS station, but when attempting to measure the state, Bob does not detect anything at his measurement station. Several events can lead to this situation, depending on whether one of the sources generated more than one photon. Therefore we must identify all of these cases. To simplify the analysis, we introduce the notation P_{ijkl}

$P(A=x,B=y)$	$P(A=x,B=\emptyset)$		$P(A=\emptyset,B=y)$		$P(A=\emptyset,B=\emptyset)$	
P_{2110}	$P_{2200,SD}$		$P_{2020,SD}$		P_{2002}	$P_{2020,DD}$
	P_{2101}		P_{2011}		P_{3001}	
	P_{3100}		P_{3010}		$P_{2200,DD}$	
P_{2111}	P_{2102}	$P_{3200,SD}$	P_{2012}	$P_{3020,DD}$	P_{2003}	$P_{2030,DD}$
$P_{2210,SD}$	$P_{2201,SD}$	$P_{2120,DD}$	$P_{2021,SD}$	$P_{2210,DD}$	P_{3002}	$P_{3200,DD}$
$P_{2120,SD}$	$P_{2300,SD}$		$P_{2030,SD}$		$P_{2201,DD}$	$P_{3020,SD}$
P_{3110}	P_{3101}		P_{3011}		$P_{2021,DD}$	$P_{2300,DD}$

Table 1.1: Different contributions to the probabilities $P(A=x,B=y)$, $P(A=x,B=\emptyset)$, $P(A=\emptyset,B=y)$ and $P(A=\emptyset,B=\emptyset)$, where x and y stand for the outcome of Alice and Bob's measurement, respectively. Note that, in the case in which more than one photon is detected at the local stations, we must distinguish between them clicking at the same (denoted with subscript SD) or different (DD) detectors. The first case is seen as an acceptable outcome x or y, since we assume that detectors are not number resolving, whereas DD cases are recognized as wrong events by Alice and Bob and are thus assigned to an erroneous outcome $\emptyset$.

to denote the probability associated with each of these events. The indices stand for i photons arriving at the CHS, j and k photons being detected by Alice and Bob, respectively, and l photons lost at any point in the set-up. To first order in $g^{(2)}$ and with vacuum emission included in the local efficiency, we can restrict the analysis to total photons numbers of 4 and 5 so that $4 \leq i+j+k+l \leq 5$. Moreover, $i \geq 2$, since the accepted detection patterns at the CHS require two photons being detected. Table A.1 in Appendix A.4 shows all the different contributions that contribute to each probability term.

We now divide the contributions into four categories: $P(A=x,B=y)$ with $x,y=\pm 1$ includes all the terms in which both Alice and Bob measure a click in one and only one of their detectors; $P(A=x,B=\emptyset)$ and $P(A=\emptyset,B=y)$ describe events where one of them does not detect any photon and $P(A=\emptyset,B=\emptyset)$ is the probability that none of them detected anything, as specified in Table 4.1. It is important to note that when more than one photon is reflected at the first beam splitter, they can either be detected at the same (denoted with subscript SD) or different (DD) detectors. In the first situation, this probability will contribute to $P(A=x,B=\emptyset)$ and $P(A=\emptyset,B=y)$, since we assume that detectors are not number resolving and the two photons at the CHS must have originated from the same source. On the other hand, for the DD cases Alice or Bob will know that the result is incorrect. Here we will just assign it to the same category as a lost photon. Furthermore, the two photons from the other station must again have gone to the CHS and these events thus contribute to $P(A=\emptyset,B=\emptyset)$.

We start by considering the effect of multi-photon emission, in the situation typically encountered in current experiments, where the local efficiency is limited and a violation of Bell's inequality can only be obtained by post selection (thereby not closing the detection loophole). In this limit we discard all events in which Alice or Bob did not detect any photon (i.e., the probability terms $P(A=x,B=\emptyset)$, $P(A=\emptyset,B=y)$ and $P(A=\emptyset,B=\emptyset)$). Since this situation is insensitive to local losses it is desirable to set the transmittance to $T = 0.5$, which increases the heralding rate. Therefore, compared to the situation in Sec. 1.4.1, the only new contributions to the CHSH correlations are the 5-photon terms P_{2111}, P_{2210}, P_{2120} and P_{3110} (see Table A.1).

As mentioned above we will only go to lowest order in the two photon emission probability P_2 (or equivalently $g^{(2)}$ according to Eq. (2.19)). We can thus restrict the analysis to events where there are 4 and 5 photons in total and the final probability distributions are therefore given by a new probability distribution for the accepted events

$$P_T(A = x, B = y) = \frac{P_1^4 P_4(A = x, B = y) + P_1^3 P_2 P_5(A = x, B = y)}{P_1^4 + 4P_2P_1^3}, \tag{1.23}$$

where $P_4(A = x, B = y)$ and $P_5(A = x, B = y)$ correspond to the probability of 4 and 5 photon event contributions, respectively. Here $P_5(A = x, B = y)$ accounts for the possibility of any of the four single-photon sources emitting two photons. Applying Eq. (2.19) we obtain that the total probability that accounts for all the events equals

$$P_T(A = x, B = y) = \frac{P_4(A = x, B = y) + \frac{1}{2}g^{(2)} P_5(A = x, B = y)}{1 + 2g^{(2)}}. \tag{1.24}$$

This allows us to calculate the CHSH S-parameter by means of Eq. (1.4) as a function of the second order correlation function $g^{(2)}$, the efficiencies of every channel, and the indistinguishability of the photons through the moments of α_{ij} and β_{ij}.

The value of the CHSH parameter S is plotted as a function of the second order correlation function $g^{(2)}$ in Fig. 1.5. We observe a Bell violation for low values of $g^{(2)}$ that ceases once the two-photon probability exceeds a certain value of not more than 10 %. The robustness towards multi-photon contributions is dependent on the HOM visibility of the photons. The predicted values are compatible with state-of-the-art single-photon sources, where $g^{(2)} \lesssim 2\%$ is currently achieved by quantum-dot single-photon sources embedded in photonic nanostructures (Ding et al., 2016; Tomm et al., 2021; Uppu et al., 2020). In the figure we focus on the regime corresponding to a typical post-selected experiment where the local and transmission efficiencies are rather small $\eta_t = \eta_{2,1} = 0.1$. These presented results thus roughly represent the limit $\eta \to 0$. For the situations considered below with higher higher local efficiency $\eta_{2,i} \approx 1$ we find that the scheme is more robust to $g^{(2)}$.

Finally we consider the detection loophole by accepting all events (including those in which no photons are detected, i.e. $P(A = \emptyset, B = y)$, $P(A = x, B = \emptyset)$, $P(A = \emptyset, B = \emptyset)$). In the derivation of the CHSH inequality it is assumed that the measurement can only take on two values -1 and 1. Experimentally we will also have the possibility of an inconclusive outcome $\emptyset$, so we must decide on a strategy for dealing with those outcomes. Here we chose that every time Alice and Bob do not detect a photon they assign a determined outcome to it (Pironio et al., 2009) such that there are only two possible outcomes of the experiment that we can assign

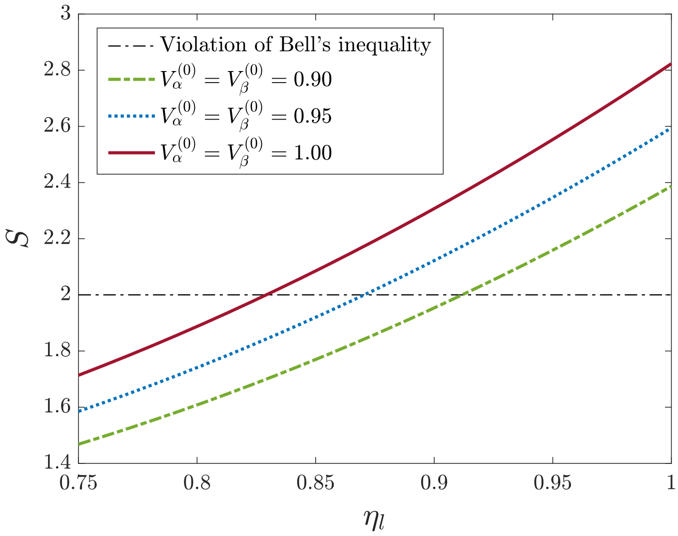


Figure 1.6: CHSH parameter S as a function of the local efficiency $\eta_l = \eta_{1,i}\eta_{2,i}(1-T)$ of Alice and Bob's stations for different HOM visibilities. To focus on the effect of the local efficiency we consider a situation with a very limited transmission to the CHS ($T = 10^{-3}$ and $\eta_t = 0.1$) and vary the efficiency of the final arm η_2 with $\eta_{1,i} = 1$.

to ± 1, as required by the CHSH inequality. In particular, Alice and Bob assign a positive detection $x, y = \{+\}$ whenever they do not detect any photon. Thus, we arrive at a probability $\tilde{P}$ distribution

$$\tilde{P}(A = x, B = y) = P(A = x, B = y) + \delta_{y,+}P(A = x, B = \emptyset) + \delta_{x,+}P(A = \emptyset, B = y) + \delta_{x,+}\delta_{y,+}P(A = \emptyset, B = \emptyset)\,. \quad (1.25)$$

This allows us to study the effect of the local efficiency on the performance of the protocol (see Fig. B.1) independently of the other effects, by setting $g^{(2)} = 0$, choosing different values of HOM visibility, and calculating the effective probabilities by applying Eq. (1.4.2) to Eqs. (1.4.2) and (1.4.2).

To mimic a situation corresponding to long distance communication where there is limited transmittance and a negligible probability to detect more than one photon at the CHS, we consider a very low transmittance of the beam splitter, $T = 10^{-3}$, and a transmittance to the CHS $\eta_t = 0.1$. We vary the local efficiency by changing the loss rate in the detection arm η_2 with $\eta_1 = 1$. These choices, however, have very little influence on the results as long as we can neglect multiphoton events at the CHS. For perfect HOM visibility, the threshold that delimits $S = 2$ is $\eta_l = 82.8\%$, which corresponds to the lowest efficiency that any CHSH Bell test can tolerate for loophole-free violation (Massar et al., 2002). The simple strategy for dealing with null detections, as introduced above, thus have similar performance as the best achievable strategy. As we introduce additional errors, see Fig. 1.7, the required local efficiency increases and goes beyond 90% for realistic values of $g^{(2)}$

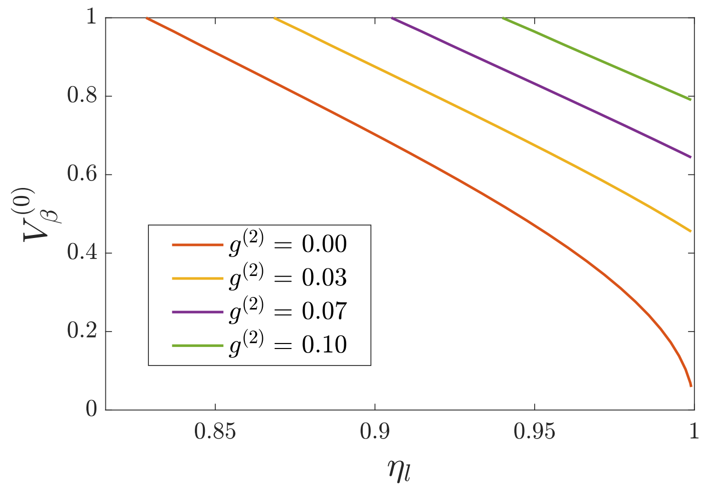


Figure 1.7: Threshold for the violation of the CHSH Bell's inequality ($S \leq 2$). We vary $\eta_{2,i}$ for different values of the second order correlation function and determine the threshold visibility $V_\beta^{(0)}$ required to violate the CHSH inequality. The local HOM visibility has been set to $V_\alpha^{(0)} = 1$ and we assume a low transmission efficiency ($T = 10^{-3}$, $\eta_t = 0.1$).

and HOM visibility. Such high local efficiency is not yet achievable in state-of-the-art implementations, although a lot of progress in this direction has been achieved in recent years (Tomm et al., 2021; Uppu et al., 2020). Note that compared to the post-selected limit (Fig. 1.5), the violation of the inequality is less sensitive to $g^{(2)}$. This is due to the difference in the local efficiency in the two plots. In the post selected limit events in which two photons are emitted have a higher chance of being accepted relative to the single-photon events, because either of the two photons can make it to the detectors. Had we considered post selection in the limit of high local efficiency, it would be less sensitive to $g^{(2)}$ since some undesired results, e.g. DD events, can be discarded.

1.4.3 Optimizing the probability of transmission T

In previous sections we have calculated and optimised the CHSH value S within the limit of a very small transmission to the CHS. This ensures a higher local efficiency and thus allows us to investigate how well the protocol might ideally work as well as identify thresholds for the success of the protocol. A low probability of transmission, however, also implies that the number of successful heralding events will be low. In this subsection we find the optimal transmittance T of the beam splitters at the local stations (see Fig. 1.1(a)) to violate Bell's inequality with the highest number of standard deviations σ_S.

The CHSH parameter (Eq. (1.20)) is the sum of four independently measured correlations $C(\mathbf{a}, \mathbf{b})$. This allows us to write the standard deviation σ_S of the CHSH

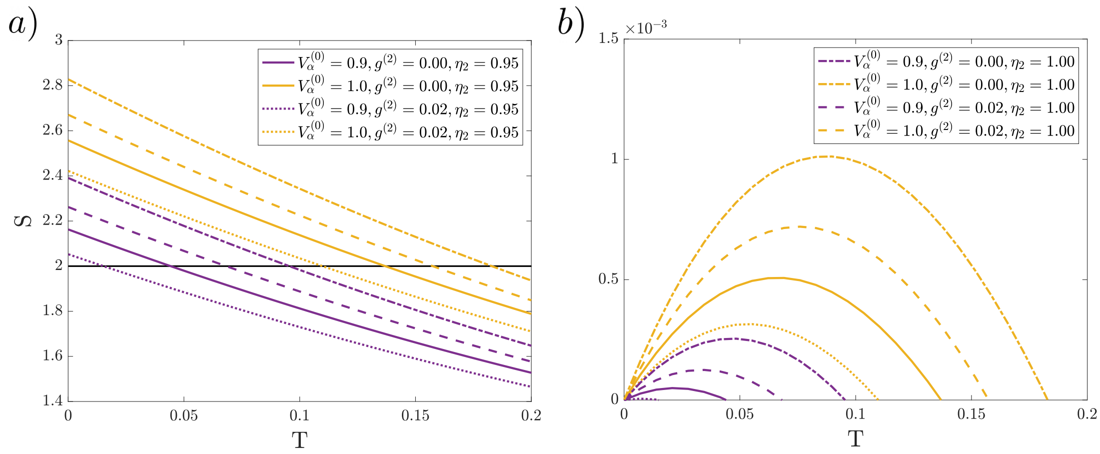


Figure 1.8: Effect of finite transmittance T. *a)* CHSH parameter S as a function of the transmittance T of the beam-splitters at the end stations for several sets of single-source error parameters: visibility ($V_\alpha^{(0)} = V_\beta^{(0)}$), purity ($g^{(2)}$), and the local efficiency (η_2 with $\eta_{1,i} = 1$). A large transmission probability decreases the performance of the protocol since there will be more events where no photons are detected at end stations. *b)* Number of standard deviations Z' with which a violation of Bell's inequality is achieved (normalised to the number of experimental runs) as a function of the transmittance T. In an experiment with n experimental runs the CHSH inequality is violated by $Z'\sqrt{n}$ standard deviations. An optimal T value that maximises the Bell violation can be found for each parameter set. Note that the legend is divided into two parts inserted in part *a)* and *b)* but applies to both subfigures *a)* and *b)*, i.e. half the lines are defined by the legend in *a)*, the others in *b)*.

parameter S as

$$\sigma_S^2 = \left\langle S^2 \right\rangle - \left\langle S \right\rangle^2 = \sigma^2_{C(\mathbf{a},\mathbf{b})} + \sigma^2_{C(\mathbf{a}',\mathbf{b})} + \sigma^2_{C(\mathbf{a},\mathbf{b}')} + \sigma^2_{C(\mathbf{a}',\mathbf{b}')} \,. \tag{1.26}$$

Furthermore, given that $C^2(\mathbf{a},\mathbf{b}) = \mathbf{a}^2\mathbf{b}^2 = 1$ we obtain the standard deviation of S for a single run of the experiment

$$\sigma_S^2 = 4 - C(\mathbf{a},\mathbf{b})^2 - C(\mathbf{a}',\mathbf{b})^2 - C(\mathbf{a},\mathbf{b}')^2 - C(\mathbf{a}',\mathbf{b}')^2 \,. \tag{1.27}$$

After a number of independent experimental runs n, there have been $N = nP_{CHS}$ successful events, where P_{CHS} is the total probability of acceptance, equal to the sum of all the probability contributions that return a positive message from the CHS. The standard deviation of the average of S yields

$$\bar{\sigma}_S = \frac{\sigma_S}{\sqrt{N/4}} = \frac{2\sigma_S}{\sqrt{nP_{CHS}}} \,, \tag{1.28}$$

where the factor of 4 arises from the four different measurement configurations of the CHSH parameter S. We define Z as the number of standard deviations with which the Bell inequality can be violated

$$Z = \frac{S-2}{\bar{\sigma}_S} = \frac{S-2}{2\sigma_S}\sqrt{nP_{CHS}}\,, \tag{1.29}$$

where we have inserted Eq. (1.28) and take into account that the violation occurs for $S > 2$.

We have optimized the set of angles for the final measurement at each station for various sets of visibility, losses and multi-photon parameters and a variable transmittance T. Using Eq. (1.29) this allows us to calculate a dimensionless number $Z' \equiv Z/\sqrt{n}$ expressing the number of standard deviations normalised by the number of experimental runs. The number of standard deviations obtained after n experimental runs is then $Z'\sqrt{n}$. As we can observe in Fig. 1.8(b), the compromise between a strong violation and the probability of success manifests itself in different optimal transmission coefficients that maximises Z' for different parameter sets. Generally the optimal transmission decreases as other errors become more significant, since in that case there is less room for errors introduced by the transmission. Furthermore, in the limit of low transmission efficiency ($\eta_t = 0.1$), the main contributions to the probability of acceptance at the CHS arise from events in which two photons arrive (and not three). This leads to $P_{CHS} \propto T^2$ resulting in a linear increase of $Z' \propto \sqrt{P_{CHS}} \propto T$ for small T, as observed in Fig. 1.8(b).

Having calculated the optimal T, it is straightforward to evaluate the number of experimental runs n necessary to violate Bell's inequality with a certain number of standard deviations Z

$$n = \left(\frac{Z}{Z'}\right)^2 . \tag{1.30}$$

Current experiments can easily reach $V_\alpha^{(0)} \geq 0.9$ and $g^{(2)} = 0.02$ (Tomm et al., 2021; Uppu et al., 2020) and for simplicity we assume that a similar visibility is reached between different stations $V_\beta^{(0)} = V_\alpha^{(0)}$. A much more challenging requirement is the local efficiency. If we assume optimistic values of $\eta_1 = 1$ and $\eta_2 = 0.95$, we get $Z' = 6.2 \cdot 10^{-6}$ with $\eta_t = 0.1$ at the optimal transmission. This means that Bell's inequality can be violated with three standard deviations after $2.3 \cdot 10^{11}$ runs. Note that for the sake of simplicity, we use the number of standard deviations with which a Bell violation is achieved as the figure of merit. For a more precise characterization of the violation in an actual experiment it would be desirable to consider the the p-value (Zhang et al., 2011). Considering the number of standard deviations, however, allows for a simpler evaluation of the requirement to achieve a violation by a different amount Z by means of Eq. (1.30).

For a typical repetition rate of the laser that excites the quantum-dot single-photon sources ($\simeq$ 75 MHz (Uppu et al., 2020; Tomm et al., 2021; Ding et al., 2016)) this approximately corresponds to only 52 minutes. If we further assume an attenuation length of 20 km, given that the data was obtained for $\eta_t = 0.1$, this allows for a separation distance between Alice and Bob's stations of more than 90 km. This is a promising result for future experimental implementations.

1.4.4 Memory considerations

For experiments based on photons emitted from a central source the locality loophole can typically be closed by rapidly switching the measurement basis at each station. The requirement for closing this loophole is then achieved by having the measurement stations sufficiently separated such that no signalling is possible, i.e. by placing the detectors outside their respective light cones.

Note, however, that for protocols based on heralding this requirement concerns the heralding station as well as Alice and Bob's stations. For photons transmitted through vacuum this can be achieved by adding only a minor delay at each station corresponding to the time it takes to detect the photons at the CHS. On the other hand if Alice and Bob are far apart it is desirable to use optical fibers for the transmission of photons between the measurement stations and the CHS. Since the speed of light is reduced when travelling in the fiber, the heralding is likely to happen inside the light cone of the stations, thus opening the locality loophole.

This problem can be solved by using local memories at the measurement stations of Alice and Bob. They would then need to store their corresponding photons until the heralding is outside the light cone. In this way, any signalling produced by the CHS would not affect the measurement of the state of the photon, thus closing the locality loophole. State-of-the-art quantum memories have reached an efficiency above 85% (Cao et al., 2020) which is in principle sufficient to allow an efficient violation using this setup, but this would put very stringent requirements on the other local efficiencies. On the other hand for the application of the considered setup for DIQKD, the locality loophole is less important and the main challenge is to close the detection loophole, which can still be achieved without memories.

1.5 Conclusion and outlook

We have studied the feasibility of using single-photon sources for loophole-free Bell test following the proposal of Kołodyński et al. (2020). The method is general and applies to any single-photon sources, but for concreteness we focus on sources based on quantum dots. Since the considered protocol is completely photonic and has a built-in robustness to losses in the transmission to the CHS, it is highly promising for violating Bell inequalities over long distances, although the reduced transmission speed of optical fibers will likely open the locality loophole for fiber based implementations. Beyond their fundamental interest such detection-loophole-free violations are of immense technological interest since they allow DIQKD, providing ultimate security in communication.

The success of the protocol is strongly dependent on the visibility, purity, and efficiency of the single-photon sources. We find that a HOM visibility of at least 79% and second-order correlation function $g^{(2)} < 10\%$ suffice for violating the CHSH inequality when post-selecting events (not loophole-free). Such metrics are already demonstrated with state-of-the-art quantum dot sources (Tomm et al., 2021; Uppu et al., 2020). Performing a fully loophole-free violation of Bell's inequality, however, remains a challenge since this puts very stringent requirements on the efficiency of the single-photon sources. For realistic parameters we find that efficiencies on the order of $\eta = 90\%$ are required. This is beyond what has been achieved so far, but continuous improvements in efficiencies have been achieved in recent years. We thus believe that sources capable of achieving such efficiencies will be available in the future. Once the necessary efficiencies are achieved it is highly encouraging that we find the requirements for the crossed visibility between stations to be lower than those for photons generated at the same station. For instance comparing Figs. 1.2 and 1.7 we see that if the local indistinguishability is high ($V_\alpha^{(0)} \approx 1$) we may obtain a violation even if the spectral fluctuations between the two quantum dots are comparable to the decay rate $\sigma \sim \gamma$. This highly relaxed performance reduces considerably the experimental complexity.

The stringent requirements on the efficiencies may be remedied by designing more advanced protocols. In particular it has been shown that by using non-maximally entangled states and Eberhard's inequality (or, equivalently, CHSH with the assignation strategy used in the present work) the efficiency threshold for Bell tests can be lowered to $\eta = 66.7\%$ (Eberhard, 1993). For the current setup such non-maximally entangled states can by obtained by replacing the beam-splitter at the CHS by a beam-splitter with a different transmission (Kołodyński et al., 2020). It is therefore very likely that a similar advantage can be gained for this system. It has, however, recently been proven that the security of some generalised DIQKD protocols involving non-maximally entangled states can be bounded to a similar threshold as the CHSH inequality (Woodhead et al., 2020; Sekatski et al., 2021). It is thus unclear if a similar advantage can also be obtained for DIQKD. In the future it will be highly interesting to explore the precise relation between the results we have obtained here and the conditions for performing DIQKD as well as the possible advantages of changing to non-maximally entangled states.

Chapter 2

Two-photon correlations for a quantum dot single-photon source

This chapter is based on selected sections from the paper in preparation Bjerlin et al. (2023)[1]. In the cited work we study the two-photon emission from a resonantly driven single quantum dot. The quantum dot is driven by a pulsed coherent field, and we find that the excitation pulse length strongly influences the properties of the quantum dot as a single-photon source. We propose a theory in which the single-photon properties are given by two effective parameters for the quantum dot, and proceed to show how two-photon bunching can be strongly suppressed by post filtering of the outgoing fields. In this chapter we showcase the pulse length's influence on the Hong-Ou-Mandel (HOM) visibility, and show how the approximation $V = 1 - F \cdot g^{(2)}$ with the commonly utilized factor $F = 2$ is incorrect in most of the short-pulse regime.

2.1 Introduction

One of the crucial components in the development of scalable photonic quantum technologies is reliable single-photon sources (Thomas et al., 2021), as argued in the Introduction. They are necessary both in the implementation of photon based optical quantum computing (Knill et al., 2001; O'brien, 2007), quantum simulation (Aspuru-Guzik et al., 2012), and long-distance quantum communication (Duan et al., 2001; Sangouard et al., 2011), with the latter point forming the bedrock of the quantum internet (Kimble, 2008). One avenue towards reliable single-photon sources are single quantum emitters, like semiconductor quantum dots (QDs) (Aharonovich et al., 2016; Senellart et al., 2017; Wang et al., 2016). Recent advances have included scalable on-demand sources with strings of more than a 100 indistinguishable

[1] With regards to the paper in preparation, the Ph.D. student participated in the discussions that shaped the final structure of the study. She derived the relation between the HOM visibility and the second order correlation function and contributed to the discussion of the rest of the results of the paper. Finally she contributed to the writing of the analysis of the relation between the HOM visibility and the second order correlation function (and the corresponding appendix) as well as the conclusion, and contributed to writing the introduction.

photons (Uppu et al., 2020). Such setups serve as likely candidates for loophole-free violation of Bell's inequality (González-Ruiz et al., 2022a) (see Chapter 1) and Device-Independent Quantum Key Distribution (González-Ruiz et al., 2022b) (see Chapter 4).

In Chapter 1 we introduced our model for a realistic quantum-dot single-photon source. This model involved using the Hong-Ou-Mandel (HOM) visibility (Hong et al., 1987) V to characterise the indistinguishability of the source, and the second-order correlation function $g^{(2)}$ to describe its purity. When studying the HOM visibility, however, we limited ourselves to only model the intrinsic visibility $V^{(0)}_{\alpha,\beta}$ of the sources, and not the effect of imperfect purity on it (see Eq. 1.10). We could not correct the effect of $g^{(2)}$ on the intrinsic visibility due to the fact that we did not study the different possible natures of the second generated photon. We model the realistic implementation of this physical setting by considering a QD that is coherently driven by a pulse of a specific length, which can leak into the detection mode with a certain probability. In addition, depending on the length of the input pulse the QD can be excited more than once, thus emitting more than a single photon.

Although the relation between HOM visibility of a source and its $g^{(2)}$ has been traditionally oversimplified to $V = V^{(0)} - 2g^{(2)}$ (Somaschi et al., 2016; Wang et al., 2019), recent work has dug into the problem for separable noise and how the indistinguishability of the extra photons emitted affects this relation (Ollivier et al., 2021). In this Chapter we extend the analysis to show the effect of the input pulse length, as well as include a more detailed description of the cause of impurity and how it influences the HOM visibility.

2.2 Analysis

In Chapter 1 we have explained how the HOM visibility of single photons provides with information about their degree of indistinguishability. We start by using the wave-function ansatz model introduced by Das et al. (2019) to model the state of the photon after the excitation of the QD, accounting for the two different mechanisms that affect the impurity mentioned above (re-excitation of the QD and leakage from the driving pulse). This ansatz is presented and motivated in detail in Bjerlin et al. (2023). It contains states for fields and emitters with up to two excitations, such that it is described by

$$\begin{aligned}\left|\tilde{\Psi}(t)\right\rangle &= c_g(t)\left|g,\varnothing\right\rangle + c_e(t)\left|e,\varnothing\right\rangle \\ &+ \int dt_e \phi_{g1}(t,t_e)\hat{E}^\dagger(v_g(t-t_e))\left|g,\varnothing\right\rangle + \int dt_e \phi_{e1}(t,t_e)\hat{E}^\dagger(v_g(t-t_e))\left|e,\varnothing\right\rangle \\ &+ \int\int dt_{e2}dt_{e1}\phi_2(t,t_{e2},t_{e1})\hat{E}^\dagger(v_g(t-t_{e2}))\hat{E}^\dagger(v_g(t-t_{e1}))\left|g,\varnothing\right\rangle ,\end{aligned} \tag{2.1}$$

with amplitudes $c_g(t)$ and $c_e(t)$ of the emitter's ground- ($|g\rangle$) and excited state ($|e\rangle$), respectively. The amplitudes $\phi_{g1}(t,t_e)$ and $\phi_{e1}(t,t_e)$ correspond to a state with one photon, emitted at a time t_e traveling in the waveguide while the emitter is in the ground state or excited state, respectively. The amplitude $\phi_2(t,t_{e2},t_{e1})$ corresponds to two emitted photons, emitted at t_{e1} and $t_{e2} > t_{e1}$, while the emitter is in the ground state. Since we only consider a maximum of two emissions, we exclude the possibility of the emitter being excited for the two-photon state. This truncation after two photon emissions is justified by considering a weak excitation field, and/or a short pulse such that the emitter does not have time to emit multiple photons[2]. We then introduce the QD decay rate Γ rescale the time to simplify the future calculations, such that $\zeta = \Gamma t$. The interaction between light and matter has been conveniently described by the slowly-varying field operator

$$\hat{E}(z) = \frac{1}{\sqrt{2\pi}} \int dk \hat{a}_k e^{i(k-k_0)z + i\omega_0 t}\,, \tag{2.2}$$

describing the annihilation of photons with wave numbers k and frequencies ω_k at a position z. This field operator obeys the commutation relation $\left[\hat{E}(z), \hat{E}^\dagger(z')\right] = \delta(z-z')$. A fraction of the coherent input field $\mathcal{E}$ should however be included in the output field, to account for the impurity generated by the leakage. For simplicity we describe it with a simple two parameter scheme such that for the output field we include the contribution

$$\mathcal{E} \to \mathcal{E}|x|e^{-i\theta}\,. \tag{2.3}$$

The factor $|x|< 1$ is the fraction of the driving field that leaks into the waveguide, and θ is the phase shift of that the field acquired through the scattering process. In Bjerlin et al. (2023) we detail how we transform the output field as it becomes a combination of the field scattered by the emitter in the transformed picture and the incident field $\hat{E} \to \hat{E} + \mathcal{E}$ (see Fig. [X]). In the complete study, we further apply different filters to the output field and study their effect. For what concerns this chapter, we are interested in the two main parameters that affect the measured purity of the source: the leakage factor $x = |x|e^{-i\theta}$ and the rescaled total pulse length ξ_T.

2.2.1 HOM Visibility

In order to calculate the HOM visibility we consider a 50:50 beam splitter with input modes $\hat{a}_1$ and $\hat{a}_2$, and output modes $\hat{a}_3$ and $\hat{a}_4$. The probability of detecting coincidence counts P_{cc} in both output ports simultaneously is given by

$$P_{cc} = \left\langle \hat{a}_3^\dagger(\zeta_e)\hat{a}_3(\zeta_e)\hat{a}_4^\dagger(\zeta_e')\hat{a}_4(\zeta_e') \right\rangle\,, \tag{2.4}$$

[2]This latter point will be revisited in later sections where we calculate two-photon correlations.

which allows us to obtain the visibility as (Brańczyk, 2017)

$$V = 1 - \frac{P_{cc}}{P_{cc,dist}}\,, \tag{2.5}$$

where $P_{cc,dist}$ is the maximum coincidence counts probability achievable, that is, for completely distinguishable extra photons.Note that we have assumed that the good single-photons from the QD are indistinguishable between them ($V^{(0)} = 1$). Applying the usual 50:50 beam splitter transformations

$$\hat{a}_1^\dagger \to \frac{1}{\sqrt{2}}\left(i\hat{a}_3^\dagger + \hat{a}_4^\dagger\right), \quad \hat{a}_2^\dagger \to \frac{1}{\sqrt{2}}\left(\hat{a}_3^\dagger + i\hat{a}_4^\dagger\right)\,, \tag{2.6}$$

and the commutation relations $[\hat{a}_i(\zeta_e), \hat{a}_j^\dagger(\zeta_e')] = \delta_{ij}\delta(\zeta_e - \zeta_e')$ for the annihilation operators to Eq.2.4 we obtain the probability of coincidence counts as a function of the input operators

$$\begin{aligned} P_{cc} = \frac{1}{4}\Big(&\left\langle \hat{a}_1^\dagger(\zeta_e)\hat{a}_1^\dagger(\zeta_e')\hat{a}_1(\zeta_e')\hat{a}_1(\zeta_e)\right\rangle + \left\langle \hat{a}_2^\dagger(\zeta_e)\hat{a}_2^\dagger(\zeta_e')\hat{a}_2(\zeta_e')\hat{a}_2(\zeta_e)\right\rangle \\ &+2\left\langle \hat{a}_1^\dagger(\zeta_e)\hat{a}_1(\zeta_e)\hat{a}_2^\dagger(\zeta_e')\hat{a}_2(\zeta_e')\right\rangle - 2\left\langle \hat{a}_1^\dagger(\zeta_e)\hat{a}_2^\dagger(\zeta_e')\hat{a}_1(\zeta_e')\hat{a}_2(\zeta_e)\right\rangle \Big)\,. \end{aligned} \tag{2.7}$$

As we can see, the first two terms are related to the unnormalised second order correlation function $G^{(2)}$ of the input fields

$$G^{(2)}\left(\zeta_T, \zeta_{e1}, \zeta_{e2}\right) = \left\langle \tilde{\Psi}(\zeta_T)\right| \hat{a}^\dagger(\zeta_{e1})\hat{a}^\dagger(\zeta_{e2})\hat{a}(\zeta_{e2})\hat{a}(\zeta_{e1}) \left|\tilde{\Psi}(\zeta_T)\right\rangle\,, \tag{2.8}$$

while the last two are connected to the first order correlation function $G^{(1)}$

$$G^{(1)}\left(\zeta_T, \zeta_{e1}, \zeta_{e2}\right) = \left\langle \tilde{\Psi}(\zeta_T)\right| \hat{a}^\dagger(\zeta_{e1})\hat{a}^\dagger(\zeta_{e2}) \left|\tilde{\Psi}(\zeta_T)\right\rangle\,. \tag{2.9}$$

Thus P_{cc} yields

$$\begin{aligned} P_{cc} = \frac{1}{4}\iint d\zeta_e d\zeta_e' \Big(&G_1^{(2)}(\zeta_e, \zeta_e') + G_2^{(2)}(\zeta_e, \zeta_e') \\ &+ 2G_1^{(1)}(\zeta_e, \zeta_e)G_2^{(1)}(\zeta_e', \zeta_e') - 2G_1^{(1)}(\zeta_e, \zeta_e')G_2^{(1)}(\zeta_e', \zeta_e)\Big)\,. \end{aligned} \tag{2.10}$$

Note that the last term in Eq. 2.10 indicates the level of indistinguishability of the photons, while the others refer to the usual one and two-photon correlations. On the other hand, we obtain $P_{cc,dis}$ taking Eq. (2.10) in the limit where $G_i^{(1)}(\zeta_e', \zeta_e') = 0$ for $i = 1, 2$:

$$P_{cc,dist} = \frac{1}{4}\iint d\zeta_e d\zeta_e' (G_1^{(2)}(\zeta_e, \zeta_e') + G_2^{(2)}(\zeta_e, \zeta_e') + 2G_1^{(1)}(\zeta_e, \zeta_e)G_2^{(1)}(\zeta_e', \zeta_e'))\,. \tag{2.11}$$

If we assume the sources to be identical for both of the input ports of the beam splitter (meaning $G_1^{(1)} = G_2^{(1)} \equiv G^{(1)}$ and $G_1^{(2)} = G_2^{(2)} \equiv G^{(2)}$), from Eqs. 2.10 and

2.11 we obtain that the HOM visibility yields

$$V = \frac{\iint d\zeta_e d\zeta_e' \left| G^{(1)}(\zeta_e, \zeta_e') \right|^2}{\iint d\zeta_e d\zeta_e' \left(G^{(2)}(\zeta_e, \zeta_e') + G^{(1)}(\zeta_e, \zeta_e) G^{(1)}(\zeta_e', \zeta_e') \right)}, \tag{2.12}$$

which we will analyse further in the following section.

2.2.2 Bounds on the relation between HOM visibility and purity

We start by describing the multiphoton state. The density matrix is

$$\hat{\rho} = \sum_i P_i \left| i \right\rangle \left\langle i \right| = P_0 \left| \emptyset \right\rangle \left\langle \emptyset \right| + P_1 \left| 1 \right\rangle \left\langle 1 \right| + P_2 \left| 2 \right\rangle \left\langle 2 \right| + ... \tag{2.13}$$

where $\sum_i P_i = 1$ holds. We consider the probability generation of three or more simultaneous photons very small, thus truncating the sum as $\hat{\rho} = P_0\hat{\rho}_0 + P_1\hat{\rho}_1 + P_2\hat{\rho}_2$, where we have defined the vacuum term as $\hat{\rho}_0 \equiv \left| \emptyset \right\rangle \left\langle \emptyset \right|$, the single-photon term as

$$\hat{\rho}_1 = \iint dt_1 dt_2 \psi^*(t_1)\psi(t_2)\hat{a}^\dagger(t_1) \left| \emptyset \right\rangle \left\langle \emptyset \right| \hat{a}(t_2)\,, \tag{2.14}$$

and the two-photon term:

$$\hat{\rho}_2 = \frac{1}{N_2} \iiiint dt_1 dt_2 dt_3 dt_4 \phi^*(t_1)\zeta^*(t_2)\phi(t_3)\zeta(t_4)\hat{a}^\dagger(t_1)\hat{a}^\dagger(t_2) \left| \emptyset \right\rangle \left\langle \emptyset \right| \hat{a}(t_3)\hat{a}(t_4)\,, \tag{2.15}$$

where $N_2 = 1 + \iint dt_1 dt_2 \phi^*(t_1)\phi(t_2)\zeta^*(t_2)\zeta(t_1)$ by normalisation (we claim that all the spectral distributions are normalized: $\int_{-\infty}^{\infty} |f(t)|^2 dt = 1$). On the other hand, the second order correlation function $g^{(2)}$ is given by:

$$g^{(2)} = \frac{\iint d\tau_1 d\tau_2 G^{(2)}(\tau_1, \tau_2)}{\iint d\tau_1 d\tau_2 G^{(1)}(\tau_1, \tau_1) G^{(1)}(\tau_2, \tau_2)} = \frac{\left\langle \iint d\tau_1 d\tau_2 \hat{a}^\dagger(\tau_1)\hat{a}^\dagger(\tau_2)\hat{a}(\tau_2)\hat{a}(\tau_1) \right\rangle}{\left\langle \int d\tau_1 \hat{a}^\dagger(\tau_1)\hat{a}(\tau_1) \right\rangle \left\langle \int d\tau_2 \hat{a}^\dagger(\tau_2)\hat{a}(\tau_2) \right\rangle}\,. \tag{2.16}$$

Let us calculate each of the expectation values independently. We start by calculating:

$$\begin{aligned} \int d\tau_1 G^{(1)}(\tau_1, \tau_1) &= \left\langle \int d\tau_1 \hat{a}^\dagger(\tau_1)\hat{a}(\tau_1) \right\rangle \\ &= \mathrm{Tr}\left\{ (P_0\hat{\rho}_0 + P_1\hat{\rho}_1 + P_2\hat{\rho}_2) \int d\tau_1 \hat{a}^\dagger(\tau_1)\hat{a}(\tau_1) \right\} = P_1 + 2P_2\,. \end{aligned} \tag{2.17}$$

The expectation value $\left\langle \int d\tau_1 d\tau_2 \hat{a}^\dagger(\tau_1)\hat{a}^\dagger(\tau_2)\hat{a}(\tau_2)\hat{a}(\tau_1) \right\rangle$ is calculated in a very similar way. This time, only the two-photon component of the density matrix gives a non-zero contribution:

$$\iint d\tau_1 d\tau_2 G^{(2)}(\tau_1, \tau_2) = \left\langle \int d\tau_1 d\tau_2 \hat{a}^\dagger(\tau_1)\hat{a}^\dagger(\tau_2)\hat{a}(\tau_2)\hat{a}(\tau_1) \right\rangle = 2P_2\,. \tag{2.18}$$

Inserting Eqs. (2.17) and (2.18) in the definition of $g^{(2)}$ (Eq. (2.16)) we finally obtain:

$$g^{(2)} = \frac{2P_2}{(P_1 + 2P_2)^2} \simeq \frac{2P_2}{P_1^2}\,, \tag{2.19}$$

approximating to first order in P_2. Furthermore, we insert Eqs. (2.17) and (2.18) into the probabilities from Eq. (2.5) to obtain the HOM visibility as a function of the one-photon (P_1) and two-photon probabilities (P_2):

$$V = 1 - \frac{P_1^2 + 4P_1P_2 + 2P_2 - \iint d\zeta_e d\zeta_e' \left|G^{(1)}(\zeta_e, \zeta_e')\right|^2}{P_1^2 + 4P_1P_2 + 2P_2}\,. \tag{2.20}$$

We are most interested in finding the slope of the second order correlation function with regards to the HOM visibility,

$$V = 1 - Fg^{(2)} \tag{2.21}$$

which we just defined as F. We then further calculate

$$\left|G^{(1)}(t,t')\right|^2 = \left\langle \hat{a}^\dagger(t)\hat{a}(t')\right\rangle \left\langle \hat{a}^\dagger(t)\hat{a}(t')\right\rangle = \Big(P_1\psi(t)\psi^*(t')$$
$$+P_2\frac{\phi(t)\phi^*(t') + \zeta(t)\zeta^*(t') + \phi^*(t')\zeta(t)\int d\tau\phi(\tau)\zeta^*(\tau) + \phi(t)\zeta^*(t')\int d\tau\phi^*(\tau)\zeta(\tau)}{1+\int d\tau d\tau'\phi^*(\tau)\zeta^*(\tau')\phi(\tau')\zeta(\tau)}\Big)\Big(\text{C.c.}\Big)\,. \tag{2.22}$$

Now integrating over time and approximating to first order in P_2:

$$\iint dtdt'\left|G^{(1)}(t,t')\right|^2 = P_1^2 + \frac{2P_1P_2}{1+\int d\tau d\tau'\phi^*(\tau)\zeta^*(\tau')\phi(\tau')\zeta(\tau)}\cdot$$
$$\iint dtdt'\Big[\phi^*(t)\psi(t)\psi^*(t')\phi(t') + \zeta^*(t)\psi(t)\psi^*(t')\zeta(t')$$
$$+\int d\tau\Big(\psi^*(t')\zeta(t')\phi^*(t)\psi(t)\zeta^*(\tau)\phi(\tau) + \psi^*(t')\phi(t')\zeta^*(t)\psi(t)\phi^*(\tau)\zeta(\tau)\Big)\Big]\,, \tag{2.23}$$

so that we can fully calculate Eq. 2.20.

Indistinguishable photons

If all photons from the single-photon sources are indistinguishable, then so are their spectral functions $\psi(t) = \phi(t) = \zeta(t)$. Thus

$$\iint dtdt'\left|G^{(1)}(t,t')\right|^2 = P_1^2 + \frac{2P_1P_2}{1+\int d\tau d\tau'\psi^*(\tau)\psi^*(\tau')\psi(\tau')\psi(\tau)}\cdot$$
$$\iint dtdt'\Big[\psi^*(t)\psi(t)\psi^*(t')\psi(t') + \psi^*(t)\psi(t)\psi^*(t')\psi(t')$$
$$+\int d\tau\Big(\psi^*(t')\psi(t')\psi^*(t)\psi(t)\psi^*(\tau)\psi(\tau) + \psi^*(t')\psi(t')\psi^*(t)\psi(t)\psi^*(\tau)\psi(\tau)\Big)\Big]$$
$$= P_1^2 + \frac{2P_1P_2}{2}(1+1+1+1)) = P_1^2 + 4P_1P_2\,, \tag{2.24}$$

and therefore the visibility yields

$$V = 1 - \frac{2P_2}{P_1^2 + 4P_1P_2 + 2P_2} \simeq 1 - \frac{2P_2}{P_1^2} = 1 - g^{(2)} \to F = 1\,. \tag{2.25}$$

However, in case we consider a coherent state, then $P_1^2 \approx 2P_2$. Then

$$V_{\text{coh}} \simeq 1 - \frac{2P_2}{P_1^2 + 2P_2} \approx 1 - \frac{2P_2}{2P_1^2} = 1 - \frac{g^{(2)}}{2} \to F_{\text{coh}} = \frac{1}{2}\,. \tag{2.26}$$

This result agrees with the fact that $g^{(2)} = 1$ for a coherent pulse.

Secondly emitted photons are distinguishable from the others

The extra photons are distinguishable from the good single-photons. All the extra photons are however identical, then $\psi(t) = \phi(t)$ holds. Thus

$$\iint dtdt' \left| G^{(1)}(t,t') \right|^2 = P_1^2 + 2P_1P_2\,, \tag{2.27}$$

and the visibility for both the single-photon and coherent case:

$$\begin{aligned} V &\simeq 1 - \frac{(1+P_1)\,2P_2}{P_1^2} = 1 - (1+P_1)\,g^{(2)} \to F = 1 + P_1 \\ V_{\text{coh}} &\approx 1 - \frac{(1+P_1)\,2P_2}{2P_1^2} = 1 - \frac{(1+P_1)}{2} g^{(2)} \to F_{\text{coh}} = \frac{1+P_1}{2}\,. \end{aligned} \tag{2.28}$$

For a good single-photon source P_1 is close to 1, and therefore $F \approx 2$. It is in this case (and only under these conditions) that the HOM visibility can be expressed as $V = 1 - 2g^{(2)}$, as usually expressed in the single-photon source community.

All photons are distinguishable

Finally if all photons are distinguishable, then $\psi(t) \neq \phi(t) \neq \zeta(t)$ holds. Thus

$$\iint dtdt' \left| G^{(1)}(t,t') \right|^2 = P_1^2\,, \tag{2.29}$$

such that the distinguishability term only has the one-photon contribution. Then the visibilities reduce to

$$\begin{aligned} V &\simeq 1 - \frac{(1+P_1)\,2P_2}{P_1^2} = 1 - (1+2P_1)\,g^{(2)} \to F = 1 + 2P_1 \\ V_{\text{coh}} &\approx 1 - \frac{(1+2P_1)\,2P_2}{2P_1^2} = 1 - \frac{(1+2P_1)}{2} g^{(2)} \to F_{\text{coh}} = \frac{1+2P_1}{2}\,, \end{aligned} \tag{2.30}$$

which again for good single-photon sources ($P_1 \approx 1$) means that $F = 3$.

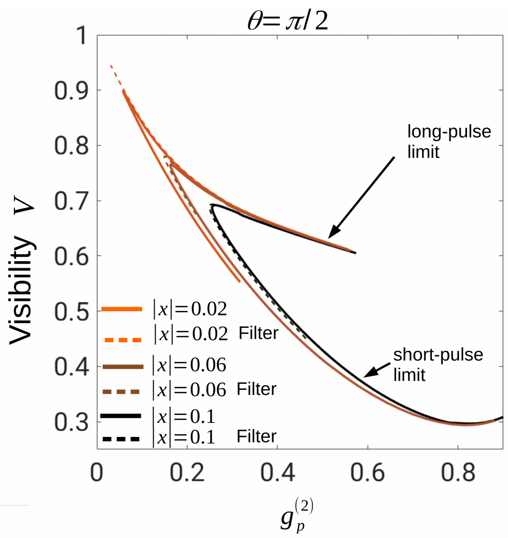


Figure 2.1: HOM visibility of QD in a leaky waveguide with phase shift $\theta = \pi/2$, representing an estimate of the average phase, at different pulse lengths, plotted against the corresponding value of $g^{(2)}$. The functions are multivalued, since the visibility is reduced both in the long- and the short-pulse limit. The turning point corresponds to the maximum visibility and the minimum in $g^{(2)}$.

2.3 Results

To investigate the relation between the two-photon correlations and visibility, we consider the factor F, implicitly defined through $V = 1 - F \cdot g^{(2)}$ (see Fig. 2.1). This factor is commonly employed in visibility calculations to account for the reduction in visibility due to two-photon pollution from single-photon sources. As shown in the previous section, the factor can be approximated by assuming a certain distinguishability between the main single-photon components and the additional photons. For a more realistic model of the single-photon source, however, the true relations can be calculated directly from computing $F = (1 - V)/g^{(2)}$. This gives insight into the subtle interplay between pulse length, two-photon pollution, and visibility.

In Fig. 2.2, the factor F is calculated for three different leakage factors $|x|$ over a range of phases and pulse lengths. We first note the behavior of the factor for $\theta = 0$, which is strongly peaked around a pulse length that corresponds to the minimum of $g^{(2)}$. This is an effect of interference between the leaked field and the field emitted by the QD. For the other phases, the factor is bounded so that $F < 3$. This indicates that in the maximally distinguishable limit, where the second emitted photon has minimal overlap with the first emitted photon, one should estimate $V = 1 - 3 \cdot g^{(2)}$. It is also clear that the effective factor is increased by the application of a filter in the short-pulse limit. This can be interpreted as the filter increasing the distinguishablility of first and second emitted photons, since higher F equals higher distinguishability. An explanation of this behavior is that both the single- and two-photon components of the leaked field are filtered out in the short-pulse

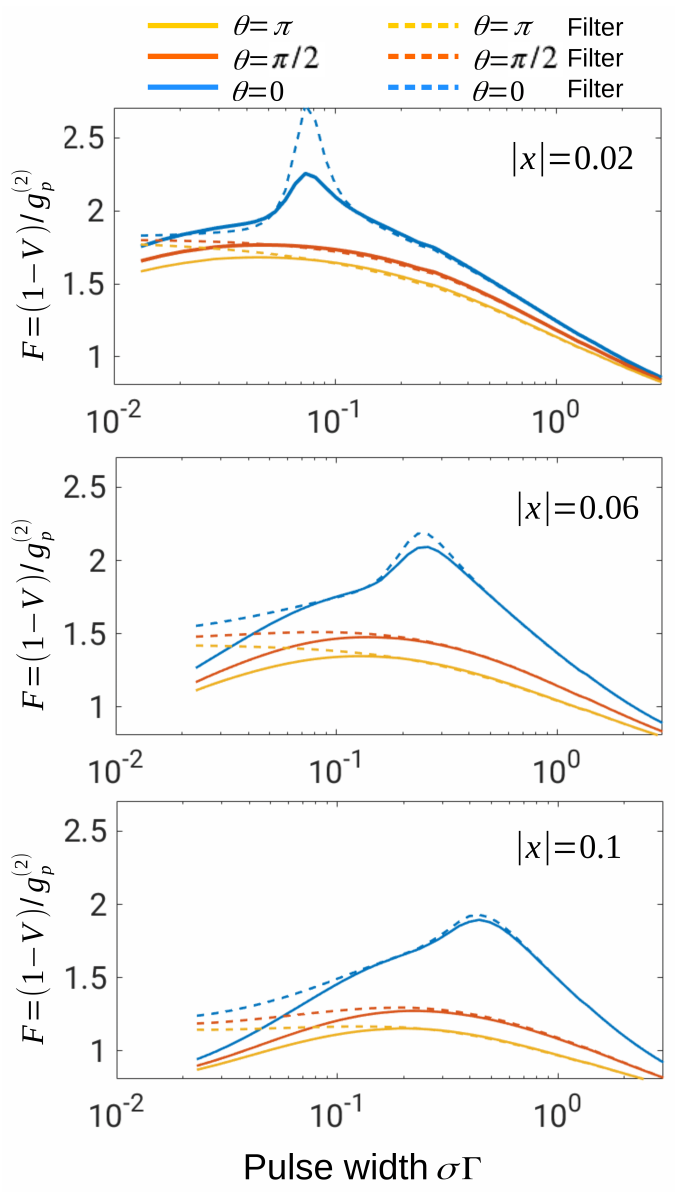


Figure 2.2: Factor $F = (1 - V)/g^{(2)}$ at different pulse lengths. The factor F represents a commonly utilized parameter used to estimate the intrinsic visibility $V^{(0)}$ of single-photon sources from measurements of V and $g^{(2)}$. The measured factor varies across different pulse lengths, phases and leakage fractions $|x|$, so should therefore not be approximated as constant by default.

limit. Photons remain distinguishable to a larger extent since the QD single photon remains in the output. At some short pulse the entire leaked field is filtered out, and the two-photon component is lost. At this point F becomes undefined.

2.4 Conclusions and Outlook

We have studied the two-photon correlations of a quantum-dot single-photon source placed in a leaky waveguide when excited by a coherent field. We study the relation between the second order correlation function $g^{(2)}$ and the HOM visibility V. Contrary to the common representation in the literature of $F = (1 - V)/g^{(2)} = 2$, the factor F is in fact bounded between $F \in [1, 3]$ for single photon sources depending on the degree of photon distinguishability. The distinguishability of the interfered photons will depend on the mechanism that reduces the purity of the sources, and thus the input pulse length. By choosing the pulse length at which $g^{(2)}$ is minimum, we see how the HOM visibility can be maximised, which we explored the importance of in Chapters 1 and further in 4.

Chapter 3

Entanglement properties of a quantum-dot biexciton cascade in a chiral nanophotonic waveguide

This chapter is based on the preprint González-Ruiz et al. (2023)[1]. We analyse the entanglement properties of deterministic path-entangled photonic states generated by coupling the emission of a quantum-dot biexciton cascade to a chiral nanophotonic waveguide, as implemented by Østfeldt et al. (2022). We model the degree of entanglement through the concurrence of the two-photon entangled state in the presence of realistic experimental imperfections. The model accounts for imperfect chiral emitter-photon interactions in the waveguide and the asymmetric coupling of the exciton levels introduced by fine-structure splitting along with time-jitter in the detection of photons. The analysis shows that the approach offers a promising platform for deterministically generating entanglement in integrated nanophotonic systems in the presence of realistic experimental imperfections.

3.1 Introduction

The generation of high-fidelity entanglement is key for the development of modern quantum technologies (Horodecki et al., 2009; Jozsa et al., 2003). Entangled states of photons have been widely generated probabilistically by employing spontaneous parametric down-conversion (SPDC) (Zhong et al., 2018), but the probabilistic nature of this process is a major obstacle for scaling up to high photon numbers. The possibility of entanglement generation on demand is of utmost importance for a wide range of quantum information applications, such as measurement-based quan-

[1]The paper contains a theoretical investigation of an experiment carried out in the quantum Photonics group (Østfeldt et al., 2022). The Ph.D. student participated in the planning of how the analysis would be structured. She did the theoretical analysis and modelling under the supervision of AS. FT, RU and PL designed the experimental implementation of the system and contributed with relevant discussions of the theoretical analysis. The Ph.D. student wrote the first version of the complete manuscript and contributed to the posterior revisions.

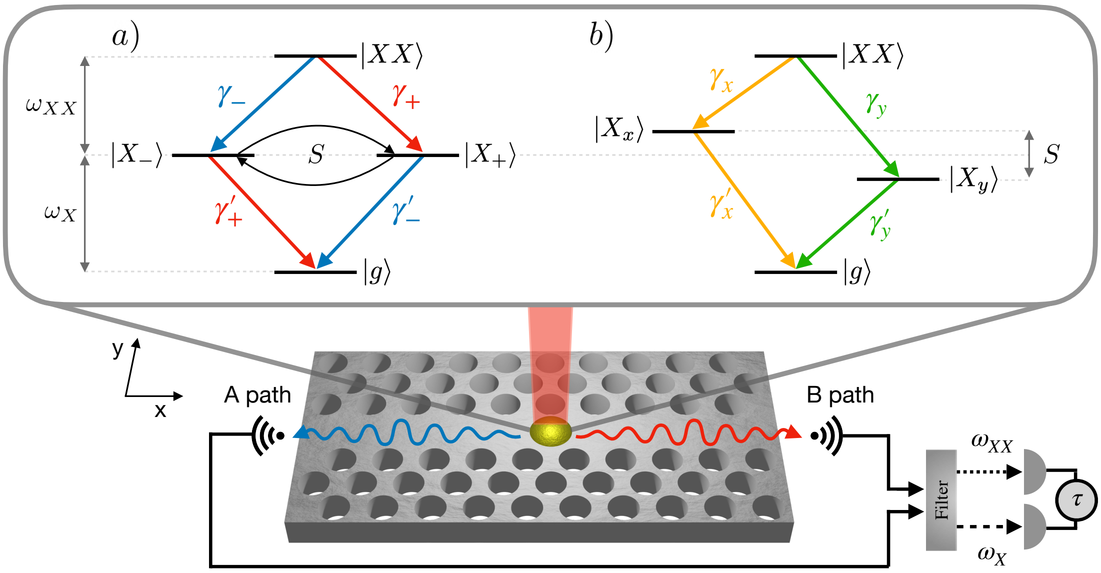


Figure 3.1: Entanglement generation scheme and level structure of the quantum dot (QD). The QD (yellow semisphere) is placed in a chiral nanowaveguide, and is excited from above, perpendicularly to the nanostructure plane. The photons emitted by the QD can couple to the left (A path) or to the right (B path). The light is collected and frequency-filtered to separate between the biexciton (ω_{XX}) and exciton (ω_X) photons in order to measure the desired temporal correlations as a function of τ, the difference between the two emission times. The level structure of the QD can be expressed in two different bases: a) *Circular basis.* The biexciton level $|XX\rangle$, with energy $\hbar\omega_{XX}$, emits two opposite circularly-polarised photons (circular right and left polarised with $\gamma_\pm$ decay rates, respectively). In this picture, the two exciton levels $|X_+\rangle$ and $|X_-\rangle$ have the same energy $\hbar\omega_X$, but are coupled at a frequency equal to the fine-structure splitting S, which makes the state time-dependent. The exciton $|X_+\rangle$ decays at rate γ'_- to the ground state $|g\rangle$, and so does $|X_-\rangle$ at a rate γ'_+. b) *Linear basis.* The biexciton level $|XX\rangle$ has the same energy as in the circular basis, but the two emitted photons have opposite linear polarisation (horizontal and vertical with γ_x and γ_y decay rates, respectively). The two exciton levels are no longer degenerate, but split into the exciton levels $|X_x\rangle$ and $|X_y\rangle$, that are stationary in time. The exciton level $|X_x\rangle$ ($|X_y\rangle$) couples to the x (y) in-plane dipole component and has energy $\omega_x + S/2$ ($\omega_x - S/2$). It decays to the ground state $|g\rangle$ at a rate γ'_x (γ'_y).

tum computing (Bartolucci et al., 2021; Briegel et al., 2009). The biexciton cascade from quantum-dot (QD) photon sources has been investigated as an on-demand entanglement generator (Benson et al., 2000; Akopian et al., 2006; Liu et al., 2019; Huber et al., 2018). The emitted states are, however, entangled in the polarisation degree of freedom, which is incompatible with implementations in integrated photonic circuits (Politi et al., 2009) that typically support only a single polarisation mode. This poses a challenge for future integration and scalability of quantum technologies (Wang et al., 2020) relying on biexciton-cascade entanglement sources.

A solution to the integration of the biexciton source into nanophotonic devices was presented in Østfeldt et al. (2022). Here the photon emission from a cascaded-biexciton decay from InGaAs quantum dots was coupled to a chiral nanophotonic waveguide (Söllner et al., 2015) (see Fig. 5.2). The polarisation-dependent directional emission enabled by chiral coupling of dipoles in these waveguides enable a promising route for on-chip, path-entangled photon generation. Two-photon excitation of the quantum dot prepares the system in the biexciton state $|XX\rangle$ with energy $\omega_{XX} + \omega_X$, which decays through two possible channels to the exciton levels $|X_\pm\rangle$ (see Fig. 5.2(a)). In a homogenous medium, the biexciton decays radiatively to one of the exciton levels, emitting a photon with either right (σ_+) or left (σ_-) circular polarisation. The two exciton levels, $|X_+\rangle$ and $|X_-\rangle$, are degenerate with energy ω_X and decay to the ground state $|g\rangle$ emitting photons with opposite circular polarisation to that emitted during the biexciton decay due to angular momentum conservation. The two emitted photons are thus entangled in polarisation as there is no information regarding which decay path the system followed. To turn this into a chip-compatible, path-entangled photon source, the QD is placed in a single-mode chiral photonic crystal waveguide which allows converting the polarisation of the transition dipole moment to the emission direction of the photon, i.e. σ_- dipoles emit to the left (path A) and σ_+ dipoles emit to the right (path B). The polarisation entangled state created by the biexciton cascade is thus translated into path encoding that can be used in integrated photonic circuits. Østfeldt et al. (2022) reported on experimental measurements of the dynamics by out-coupling the photons from the waveguide and frequency-filtering them in order to separate photons emitted on the biexciton and exciton transitions. The desired correlations were then measured through a Hanbury-Brown-Twiss (HBT) experiment (Brown et al., 1954), as shown in Fig. 5.2.

While an ideal QD that is precisely positioned at a chiral point could generate maximally entangled, path-encoded photon pairs, imperfections in the QD as well as in the chiral coupling could impact the degree of entanglement. In particular, intrinsic asymmetry of the QD could lead to coupling between the exciton states $|X_\pm\rangle$ through a spin-flip oscillation with a frequency S that is known as the fine-structure splitting (FSS) of the QD. In this work we provide a full theoretical analysis of the entanglement properties of the path-entangled state accounting for all these imperfections. This analysis already successfully described the experimental findings in Østfeldt et al. (2022), but here we provide the full details of the theory and apply it to systematically analyse the impact of various errors on the degree of entanglement. In particular, the aforementioned FSS induces a frequency splitting of the exciton levels (see Fig. 5.2), which effectively creates a time dependence of the entangled polarisation states. This can reduce the quality of entanglement when imperfect time detection of photons is taken into account. Moreover, since the photons emitted in the two different decay paths in Fig. 5.2(b) have different polarisations, the two paths may occur with different probabilities in photonic nanostructures, given by the polarisation dependent local density of states. These effects, together with imperfect chiral coupling to the waveguide, can reduce the amount of entanglement. The analysis and understanding of these effects will be important for further explorations of the biexciton cascade as an on-demand source of path-entangled photons in integrated quantum information platforms.

3.2 Analysis

We start our analysis by introducing the Hamiltonian of the system and a wavefunction ansatz for the state generated by means of the light-mater interaction with the QD. The state is then fully characterised through studying its evolution by solving Schrödinger's equation.

3.2.1 The Hamiltonian and wavefunction ansatz

The biexciton level structure can be expressed in two different bases. In the linear polarisation basis (Fig. 5.2(b)), the emitted photons are linearly polarised (either horizontally or vertically, with γ_x and γ_y decay rates, respectively), while in the circular basis (Fig. 5.2(a)) the photons are circularly polarised (with right- and left-circularly polarised photons, and γ_+ and γ_- decay rates, respectively). In the linear basis the two exciton levels have different energies, split by the FSS S, while in the circular basis the levels are degenerate. In the latter basis, there is a time-dependent oscillation between the two exciton levels at a frequency S.

The full system is described by the total Hamiltonian $\hat{H} = \hat{H}_0 + \hat{H}_f + \hat{H}_{int}$, which can be decomposed into the free energy of the emitter- $\hat{H}_0$, the free field- $\hat{H}_f$ and the interaction $\hat{H}_{\text{int}}$ Hamiltonians. These are given by

$$\begin{aligned}
\hat{H}_0 &= \hbar\left(\omega_{XX} + \omega_X\right)|XX\rangle\langle XX| + \hbar\left(\omega_X + \frac{S}{2}\right)|X_x\rangle\langle X_x| \\
&\qquad + \hbar\left(\omega_X - \frac{S}{2}\right)|X_y\rangle\langle X_y| \\
\hat{H}_f &= \hbar\int\left(\omega_{X,\mathbf{k}}\hat{a}^\dagger_{\mathbf{k}}\hat{a}_{\mathbf{k}} + \omega_{XX,\mathbf{k}}\hat{a}'^\dagger_{\mathbf{k}}\hat{a}'_{\mathbf{k}}\right)d\mathbf{k} \\
\hat{H}_{\text{int}} &= -\frac{q}{m_0}\hat{\boldsymbol{A}}\cdot\hat{\boldsymbol{p}},
\end{aligned} \tag{3.1}$$

where we have chosen the Coulomb gauge with vector potential $\mathbf{A}$. The QD is described by the coordinate $\mathbf{r}$ with the conjugate variable or generalised momentum $\mathbf{p}$, charge q and mass m_0 (Lodahl et al., 2015). Ideally, the energy of the biexciton ($|XX\rangle$) and exciton ($|X_\alpha\rangle$ with $\alpha = x, y$) levels is given by $\hbar\omega_{XX}$ and $\hbar\omega_X$, respectively. The FSS S, however, splits the exciton levels into $\hbar(\omega_X \pm S/2)$ in the linear polarisation basis. Note that we express the total Hamiltonian in a linear polarisation basis as it simplifies the temporal dynamics of the system. The field annihilation operators $\hat{a}_\mathbf{k}$ are momentum dependent, where $\mathbf{k}$ expresses the corresponding wavevector,and the prime indicates whether it annihilates a biexciton ($\hat{a}'_\mathbf{k}$) or an exciton ($\hat{a}_\mathbf{k}$) photon. The biexciton and exciton binding energies are assumed to be sufficiently different to treat them as two independent reservoirs. This assumption is motivated by the $2-3$ meV energy splitting between the exciton and biexciton binding energies observed in QDs, which is over three orders of magnitude larger than the natural linewidths of these transitions (Pedersen et al., 2020).

To put the interaction Hamiltonian into a simpler form, the conjugate variable $\mathbf{p}$ (proportional to the dipole operator) can be expressed in terms of the transition matrix elements $\hat{\mathbf{p}} = \sum_{l,m} \langle l| \hat{\mathbf{p}} |m\rangle |l\rangle \langle m|$, where the indexes l and m represent the excited and ground states of the transition, respectively. This allows us to express the interaction Hamiltonian as

$$\hat{H}_{\text{int}} = \sum_{l,m,\mathbf{k}} \langle l| \hat{\mathbf{p}} |m\rangle \cdot \mathbf{U}_{\mathbf{k}(\mathbf{r})} \hat{a}_k |l\rangle \langle m| + \text{H.c.}\,, \tag{3.2}$$

where $\mathbf{U}_{\mathbf{k}(\mathbf{r})}$ is the modefunction of the field. We consider that the field propagates in the waveguide along the x direction. Following Bloch's theorem we thus have $\mathbf{U}_k(\mathbf{r}) = \mathbf{e}_k(\mathbf{r})e^{ikx}$, where $\mathbf{e}_k(\mathbf{r})$ is the Bloch function describing the electric field with wavenumber k at the QD position $\mathbf{r}$, and the field only propagates in the x direction. Moreover we assume that the QD only interacts within a narrow frequency range around the resonance frequency with wavenumbers $\pm k_0$ yielding

$$\hat{H}_{\text{int}} = \sum_{\substack{l,m \\ k\approx\pm k_0}} \langle l| \hat{\mathbf{p}} |m\rangle \cdot \mathbf{e}_k(\mathbf{r})e^{ikx} \hat{a}_k |l\rangle \langle m| + \text{H.c.}\,, \tag{3.3}$$

where for brevity we have taken only the non primed annihilation operators, with the sign of k indicating whether the field propagates to the right ($+k_0$) or to the left ($-k_0$). By assuming the same wavenumber in both directions, we implicitly assume time-reversal symmetry for the propagation of the field in the waveguide (i.e. without the QDs). This is valid as long as we can e.g. neglect the intrinsic Faraday effect of the waveguide. Since waveguides are very broad band this is typically an excellent approximation and does not exclude any possible violation of time-reversal symmetry of the QD if an external magnetic field was applied.

The polarisation of the emitted light is determined by the symmetry of the states, which results in the following matrix elements for the dipole forbidden transitions in the linear polarisation basis

$$\langle XX| \hat{p}_x |X_y\rangle = \langle XX| \hat{p}_y |X_x\rangle = \langle X_x| \hat{p}_y |g\rangle = \langle X_y| \hat{p}_x |g\rangle = 0\,, \tag{3.4}$$

as the x (y) component of the dipole only couples to the horizontally (vertically) polarised light. Moreover, the allowed transitions from the exciton levels have a dipole moment defined as P,

$$\langle X_x| \hat{p}_x |g\rangle = \langle X_y| \hat{p}_y |g\rangle = P\,, \tag{3.5}$$

whereas the two possible biexciton decay transitions are given by (Lodahl et al., 2015)

$$\langle XX| \hat{p}_x |X_x\rangle = \langle XX| \hat{p}_y |X_y\rangle = \sqrt{2}P\,. \tag{3.6}$$

We now insert these dipole transitions in the interaction Hamiltonian from Eq. (3.3) and calculate its Fourier transform. For now we only consider the modes propagating to the right, yielding

$$\begin{aligned}\hat{H}_{\text{int}} = -P\cdot\Big[\sqrt{2}\Big(\epsilon_{k_0,x}(\mathbf{r})\,|XX\rangle\,\langle X_x| + \epsilon_{k_0,y}(\mathbf{r})\,|XX\rangle\,\langle X_y|\,\Big)e^{ik_0x_0}\hat{a}_B(x_0)\\ +\Big(\epsilon_{k_0',x}(\mathbf{r})\,|X_x\rangle\,\langle g| + \epsilon_{k_0',y}(\mathbf{r})\,|X_y\rangle\,\langle g|\,\Big)e^{ik_0x_0}\hat{a}'_B(x_0)\Big] + \text{H.c.},\end{aligned} \tag{3.7}$$

where the position-dependent annihilation operator $\hat{a}_n(x)$ is defined as

$$\hat{a}_n(x) = \frac{1}{\sqrt{2\pi}}\int_0^\infty \hat{a}_{n,\pm k}e^{i(k-k_0)x}dk\,, \tag{3.8}$$

with $n = B(A)$ denoting fields propagating to the right (left) and the sign being positive (negative) for path B (A) and x_0 is the position of the emitter. We note that since we separate the annihilation operator into left and right propagating modes (A and B) the limit of the integration is $k = 0$. In practice, however, we only expect the annihilation operator to give a contribution for $k \approx \pm k_0$. We can therefore extend the limit of integration to $-\infty$ yielding the commutator

$$[\hat{a}_n(x), \hat{a}^\dagger_{n'}(x')] = \delta_{n,n'}\delta(x-x')\,. \tag{3.9}$$

We further note that with the definition in Eq. (3.8) we make the convention that both left and right propagating fields are traveling towards positive x, i.e. the direction of the x-axis is reversed for the left propagating modes.

To relate the coupling of the right propagating modes with the left propagating modes we again invoke time-reversal symmetry of the waveguide modes. If the local electric field $\boldsymbol{\epsilon}_{k_0,x}(\mathbf{r})$ is a solution for the waveguide, then by time-reversal symmetry the solution for a wave propagating in the opposite direction is given by $\boldsymbol{\epsilon}_{-k_0}(\mathbf{r}) = \boldsymbol{\epsilon}^*_{k_0}(\mathbf{r})$. This allows us to obtain the full interaction Hamiltonian by combining Eq. (3.7) with the corresponding expression for back-propagating waves. This results in

$$\begin{aligned}\hat{H}_{\text{int}} = -\hbar\sum_\alpha\Big[\Big(g_{A,\alpha}\hat{a}_A(0) + g_{B,\alpha}\hat{a}_B(0)\Big)\,|XX\rangle\,\langle X_\alpha|\\ +\Big(g'_{A,\alpha}\hat{a}'_A(0) + g'_{B,\alpha}\hat{a}'_B(0)\Big)\,|X_\alpha\rangle\,\langle g| + \text{H.c.}\Big]\,,\end{aligned} \tag{3.10}$$

where we have set $x_0 = 0$ for simplicity and defined the complex coupling constants $g_{n,\alpha} = |g_{n,\alpha,n}|e^{i\phi_{n,\alpha}}$ and their phases in relation to the local electric field components $\epsilon_{\pm k_0,i}$ as

$$\begin{aligned}
g_{A,x} &= \sqrt{2}P\epsilon^*_{k_0,x}(\mathbf{r}), & g_{A,y} &= \sqrt{2}P\epsilon^*_{k_0,y}(\mathbf{r}), \\
g_{B,x} &= \sqrt{2}P\epsilon_{k_0,x}(\mathbf{r}), & g_{B,y} &= \sqrt{2}P\epsilon_{k_0,y}(\mathbf{r}), \\
g'_{A,x} &= P\epsilon'^*_{k_0,x}(\mathbf{r}), & g'_{A,y} &= P\epsilon'^*_{k_0,y}(\mathbf{r}), \\
g'_{B,x} &= P\epsilon'_{k_0,x}(\mathbf{r})\,. & g'_{B,y} &= P\epsilon'_{k_0,y}(\mathbf{r})\,.
\end{aligned} \tag{3.11}$$

The coupling constants in Eq. (3.11) describe the light-matter interaction between the field and the waveguide including the chirality. In particular, their magnitude describes the coupling of a horizontally or vertically polarised photon (through the x and y components of the dipole, respectively) to the left or to the right paths. From Eq. (3.11) we note that $|g_{A,\alpha}| = |g_{B,\alpha}|$ for $\alpha = x, y$, so that linearly polarized dipoles always have the same coupling constant and hence the same decay rate in both directions A and B. This does not, however, exclude that circular dipoles can have chiral interaction and predominantly decay in one direction. The existence of such chiral interactions is encoded in the relative phase of the coupling constants. From Eq. (3.11) we find that the phase difference Φ between the phases of the x and y components of the electric field is

$$\Phi \equiv \phi_x - \phi_y = \phi_{A,x} - \phi_{A,y} = -\left(\phi_{B,x} - \phi_{B,y}\right)\,, \tag{3.12}$$

and similarly for the exciton phase difference Φ'. Consider now a circularly polarized state $|X_\pm\rangle = (|X_x\rangle \pm i\,|X_y\rangle)/\sqrt{2}$. We can calculate the coupling constants $g'_{n,+}$ for the decay of these states into the $n = A, B$ directions from the interaction Hamiltonian (3.10), yielding

$$g'_{n,\pm} = \frac{1}{\sqrt{2}}(g'_{n,x} \mp i g'_{n,y})\,. \tag{3.13}$$

If $|g'_{n,x}| = |g'_{n,y}| = g'$, the decay rate of the circular states into the two directions will thus fulfill

$$\gamma'_{A,\pm} \propto |g'_{A,\pm}|^2 = g'^2(1 \pm \sin\Phi'), \quad \gamma'_{B,\pm} \propto |g'_{B,\pm}|^2 = g'^2(1 \mp \sin\Phi')\,. \tag{3.14}$$

For $\Phi' = \pi/2$ the x and y components of the field in the waveguide are phase-shifted corresponding to circular polarisation. Furthermore, whether the waveguide mode is left- or right-hand circularly polarized is linked to the propagation direction of the light. As a consequence, the system exhibits perfect chiral coupling with the circularly polarized states coupling only to a single propagation direction, i.e. $\gamma'_{A,+} \neq 0$ and $\gamma'_{B,+} = 0$, with the directions reversed for the opposite circular state. Complete absence of chirality occurs when $\Phi' = 0$, where the field in the waveguide is linearly polzarized. Thus, the parameters Φ and Φ' represent the degree of chirality of the system, which we employ in the subsequent sections of this article.

To describe the emission into the waveguide, it is convenient to change the Hamiltonian into the position basis. While the Fourier transform of the free energy term in the total Hamiltonian (3.1) is itself, Fourier transforming the free field term yields

$$\hat{H}_f = \sum_n \Big[i\hbar \int \Big(v_{gXX} \frac{\partial \hat{a}_n^\dagger(x)}{\partial x} \hat{a}_n(x) + v_{gX} \frac{\partial \hat{a}'^\dagger_n(x)}{\partial x} \hat{a}'_n(x) \Big) dx \\ + \hbar \int \Big(\omega_{X,k} \hat{a}^\dagger_{n,k} \hat{a}_{n,k} + \hbar\omega_{XX,k} \hat{a}'^\dagger_{n,k} \hat{a}'_{n,k} \Big) dk \Big], \quad (3.15)$$

where the group velocities associated with the biexciton and exciton energy levels are given by $v_{g,XX} = \partial\omega_{XX,k}/\partial k$ and $v_{g,X} = \partial\omega_{X,k}/\partial k$ respectively. Note that these two group velocities could be different due to the dispersion of the waveguide at the different emission wavelengths of the exciton and biexciton levels.

We can now write a wavefunction ansatz for the total state of the system in the real space domain. The state should describe that up to two photons can be emitted by the biexciton decay and that they couple into the left- or right-propagating waveguide modes. Based on the methods from Das et al. (2019) (with similar methods being developed in Refs. (Fischer et al., 2018; Trivedi et al., 2018; Heuck et al., 2020)) we use the following ansatz:

$$|\psi(t)\rangle = e^{-i(\omega_{XX}+\omega_X)t} \Big(c_{XX}(t) |XX\rangle |\emptyset\rangle \\ + \sqrt{v_{gXX}} \sum_{\alpha,n} \int dt_{XX} \psi_{\alpha,n}(t, t_{XX}) \hat{a}_n^\dagger(v_{gXX}(t - t_{XX})) |X_\alpha\rangle |\emptyset\rangle \\ + \sqrt{v_{gXX} v_{gX}} \sum_{n,m} \iint dt_{XX} dt_X \psi_{n,m}(t, t_{XX}, t_X) \hat{a}_n^\dagger(v_{gXX}(t - t_{XX})) \hat{a}'^\dagger_m(v_{gX}(t - t_X)) |g\rangle |\emptyset\rangle \Big), \quad (3.16)$$

where t_X and t_{XX} are the two emission times with $t_{XX} < t_X$. This state describes that with an amplitude $c_{XX}(t)$ the system is in the biexciton state with the field being in the vacuum state $|\emptyset\rangle$. Since the system is initially excited to this state we have $c_{XX}(t = 0) = 1$. The amplitude $\psi_{\alpha,n}(t, t_{XX})$ describes the state after the emission of a photon in the direction $n = A, B$ at time t_{XX} by the decay into the exciton state $|X_\alpha\rangle$. Since the photon propagates in the waveguide, this is associated with a photon at position $x = v_{gXX}(t - t_{XX})$. As this state still evolves in time the amplitude has an explicit dependence on time t with the amplitude vanishing before the emission, $\psi_{\alpha,n}(t, t_{XX}) = 0$ if $t \leq t_{XX}$. Finally, after the emission of both photons, the system is in the ground state $|g\rangle$ and the two photons are emitted in directions n, m with amplitude $\psi_{n,m}(t, t_{XX}, t_X)$. This amplitude vanishes unless $t \geq t_X \geq t_{XX}$. It should be noted that both for the left and right propagation directions in the waveguide $x \in [0, \infty]$, i.e. the reference frame is placed such that in both directions x is positive after the QD.

3.2.2 Solving the Schrödinger equation

The wavefunctions $|\psi(t)\rangle$ from Eq. (3.16) should be calculated to describe the state. We thus apply Schrödinger's equation $i\hbar\partial\,|\psi\rangle\,/\partial t = \hat{H}\,|\psi\rangle$ to the wavefunction ansatz using the space-domain Hamiltonian. Following the procedure from Das et al. (2019), we obtain the set of coupled differential equations:

$$\begin{aligned}
\dot{c}_{XX}(t) &= -\frac{i}{\sqrt{v_{gXX}}\hbar}\sum_{\alpha,n} g_{\alpha,n}\psi_{\alpha,n}(t,t), \\
\dot{\psi}_{x,n}(t,t_{XX}) &= \frac{iS}{2\hbar}\psi_{x,n}(t,t_{XX}) - \frac{ig^*_{x,n}c_{XX}(t)}{\sqrt{v_{gXX}}\hbar}\delta(t-t_{XX}), \\
&\quad - \frac{i}{\sqrt{v_{gX}}\hbar}\sum_m g'_{x,n}\psi_{n,m}(t,t_{XX},t), \\
\dot{\psi}_{y,n}(t,t_{XX}) &= -\frac{iS}{2\hbar}\psi_{y,n}(t,t_{XX}) - \frac{ig^*_{y,n}c_{XX}(t)}{\sqrt{v_{gXX}}\hbar}\delta(t-t_{XX}) \\
&\quad - \frac{i}{\sqrt{v_{gX}}\hbar}\sum_m g'_{y,n}\psi_{n,m}(t,t_{XX},t), \\
\dot{\psi}_{n,m}(t,t_{XX},t_X) &= -\frac{i}{\sqrt{v_{gX}}\hbar}\sum_{\alpha} g'^*_{\alpha,n}\psi_{\alpha,n}(t,t_{XX})\delta(t-t_X)\,.
\end{aligned} \tag{3.17}$$

We then apply the Laplace transform to the nine equations in Eq. (3.17), with the system initially prepared in the biexciton state ($c_{XX}(t=0)=1$). Inverting the Laplace transformation now yields

$$\begin{aligned}
\dot{\psi}_{x,n}(t,t_{XX}) &= -\frac{ig^*_{x,n}c_{XX}(t)}{\sqrt{v_{gXX}}\hbar}\delta(t-t_{XX}) \\
&\qquad - \left(\frac{-iS+\gamma'_x}{2\hbar}\right)\psi_{x,n}(t,t_{XX}) - \frac{\Gamma}{2\hbar}\psi_{y,n}(t,t_{XX}) \\
\dot{\psi}_{y,n}(t,t_{XX}) &= -\frac{ig^*_{y,n}c_{XX}(t)}{\sqrt{v_{gXX}}\hbar}\delta(t-t_{XX}) \\
&\qquad - \left(\frac{iS+\gamma'_y}{2\hbar}\right)\psi_{y,n}(t,t_{XX}) - \frac{\Gamma^*}{2\hbar}\psi_{x,n}(t,t_{XX})\,,
\end{aligned} \tag{3.18}$$

with the spontaneous emission rates given by

$$\gamma^{(\prime)}_{\alpha} = \sum_n \gamma^{(\prime)}_{\alpha,n} \equiv \sum_n \frac{|g^{(\prime)}_{\alpha,n}|^2}{v_{gX}}\,. \tag{3.19}$$

A coupling between the $|X_x\rangle$ and $|X_y\rangle$ states mediated by the local electric field of the waveguide is captured by the cross terms with coupling coefficient

$$\Gamma = \frac{g'_{A,x}{g'}^*_{A,y} + g'_{B,x}{g'}^*_{B,y}}{v_{gX}}\,, \tag{3.20}$$

which is real due to time-reversal symmetry (3.11). This coupling is important if e.g. the local electric field in the waveguide is diagonally polarized, which leads to $\Gamma = \gamma'_x = \gamma'_y$.

When solving the coupled set of differential equations (3.18) it is convenient to work in a basis that diagonalizes the dynamics, i.e. where the equations decouple. For a rotationally symmetric system, this is the case for any basis, but it is no longer the case once the symmetry is broken. The FSS is induced by the asymmetry of the QD and is assumed to be in the x and y-directions such that Eqs. (3.18) decouple in that basis. On the other hand, the local waveguide field may have a different orientation, which also breaks the symmetry and thus leads to a coupling between the equations, i.e. $\Gamma \neq 0$. In practice, however, we typically have $S \gg \Gamma$, e.g. in the experimental implementation in Østfeldt et al. (2022) the fine structure splitting S was an order of magnitude larger than the exciton emission rate $(\gamma'_x + \gamma'_y)/2$. The coupling between the exciton levels ($|X_x\rangle$ and $|X_y\rangle$) can therefore be neglected and we set $\Gamma = 0$. We note that this assumption may lead to inconsistencies in the obtained results due to incorrect normalization of the state in QDs with small FSS, i.e., S comparable to $(\gamma'_x+\gamma'_y)/2$. In the subsequent sections, we use $S = 4(\gamma'_x+\gamma'_y)/2$ for which we find that the magnitude differs from unity by <6%.

We now solve the two coupled differential equations from Eq. (3.18) by taking the aforementioned limit $\Gamma = 0$, such that the equations decouple. We can then straightforwardly solve them by again applying the Laplace transform, obtaining

$$\begin{aligned}
c_{XX}(t) &= e^{-\frac{1}{2\hbar}(\gamma_x+\gamma_y)t} \\
\psi_{x,n}(t,t_{XX}) &= -i\sqrt{\gamma_{x,n}}e^{-\frac{1}{2\hbar}(\gamma_x+\gamma_y)t_{XX}-\frac{1}{2\hbar}(\gamma'_x+iS)(t-t_{XX})-i\phi_{x,n}}\theta(t-t_{XX}) \\
\psi_{y,n}(t,t_{XX}) &= -i\sqrt{\gamma_{y,n}}e^{-\frac{1}{2\hbar}(\gamma_x+\gamma_y)t_{XX}-\frac{1}{2\hbar}(\gamma'_x-iS)(t-t_{XX})-i\phi_{y,n}}\theta(t-t_{XX}) \\
\psi_{n,m}(t,t_{XX},t_X) &= -e^{-\frac{1}{2\hbar}(\gamma_x+\gamma_y)t_{XX}}\Bigg(\sqrt{\gamma_{x,n}\gamma'_{x,m}}e^{-\frac{1}{2\hbar}(\gamma'_x+iS)(t_X-t_{XX})-i\left(\phi_{x,n}+\phi'_{x,m}\right)} \\
&\quad + \sqrt{\gamma_{y,n}\gamma'_{y,m}}e^{-\frac{1}{2\hbar}\left(\gamma'_y-iS\right)(t_X-t_{XX})-i\left(\phi_{y,n}+\phi'_{y,m}\right)}\Bigg)\theta(t-t_X)\theta(t_X-t_{XX})\,.
\end{aligned} \tag{3.21}$$

We now calculate the probability of detecting two photons simultaneously at the output of the waveguide in order to analyse the quality of the entanglement. To do so we correlate the biexciton and exciton photons with a time delay τ in two different settings: when both are coupled to the forward or back-propagating direction (noted as $A_X A_{XX}$ and $B_X B_{XX}$ respectively) and when they couple to opposite directions ($A_X B_{XX}$ and $B_X A_{XX}$):

$$\begin{aligned}
P_{n,m}(t,t_{XX},t_{XX}+\tau) = |v_{gXX}||v_{gX}|\langle\psi(t)|\,\hat{a}_n^\dagger(v_{gXX}t)\hat{a}_n(v_{gXX}t) \\
\cdot\,\hat{a}'^{\dagger}_m\left(v_{gX}(t-\tau)\right)\hat{a}'_m\left(v_{gX}(t-\tau)\right)|\psi(t)\rangle\;.
\end{aligned} \tag{3.22}$$

With the wavefunction ansatz Eq. (3.16) and the results from Eq. (3.21) we obtain

$$\begin{aligned} P_{n,m} &= |\psi_{n,m}(t, t_{XX}, t_{XX} + \tau)|^2 \\ &= e^{-(\gamma_x+\gamma_y)t_{XX}} \Big[\gamma_{x,n}\gamma'_{x,n} e^{-\gamma'_x \tau} + \gamma_{y,n}\gamma'_{y,n} e^{-\gamma'_y \tau} + 2\sqrt{\gamma_{x,n}\gamma_{y,n}\gamma'_{x,m}\gamma'_{y,m}}\, e^{-\frac{1}{2}(\gamma'_x+\gamma'_y)\tau} \\ &\qquad \cdot \cos\Big(S\tau + (\phi_{x,n} - \phi_{y,n}) + (\phi'_{x,m} - \phi'_{y,m})\Big)\Big] \theta(t - t_{XX} - \tau)\,. \end{aligned} \tag{3.23}$$

3.2.3 Entanglement generation

The state produced by the biexciton cascade coupled to the chiral waveguide has two different degrees of freedom: the path followed (to the left, A, or to the right, B) and the respective times of emission of the biexciton (t_{XX}) and exciton (t_X) photons. We project this state in time space by fixing the two times of detection $t_X - t_{XX} \equiv \tau > 0$. Note that the characteristics of the state produced depends only on the time difference τ.

From our wavefunction ansatz in Eq. (3.16), we post-select the two-photon emission terms by conditioning on detecting photons at times $t = t_{XX}$ and $t = t_X$, thus obtaining the state

$$|\psi(\tau)\rangle = \frac{1}{\sqrt{N}}\Big(\psi_{AA}(\tau)\,|AA\rangle + \psi_{AB}(\tau)\,|AB\rangle + \psi_{BA}(\tau)\,|BA\rangle + \psi_{BB}(\tau)\,|BB\rangle\Big)\,, \tag{3.24}$$

where,

$$N = |\psi_{AA}(\tau)|^2 + |\psi_{AB}(\tau)|^2 + |\psi_{BA}(\tau)|^2 + |\psi_{BB}(\tau)|^2\,, \tag{3.25}$$

is the normalisation factor. Note that we dropped the explicit subscripts for exciton X and biexciton XX photons on the direction index. Instead, we utilize time-ordered emission in the simplified notation, i.e. the subscript AB should be read as $A_{XX}B_X$.

In general the two possible decay channels do not have the same spontaneous emission rates, i.e., $\gamma_x \neq \gamma_y$ due to differences of the local electric field components in the waveguide. However, to achieve a high degree of chirality in the waveguide, the two exciton decay rates have to be similar $\gamma_x \approx \gamma_y$. This was also the case in the recent experiment in Østfeldt et al. (2022). For most of the article we therefore set $\gamma_x = \gamma_y$ and $\gamma'_x = \gamma'_y$, but investigate the influence of differences in the rates in Sec. 3.3.4. Moreover, the biexciton and exciton spontaneous emission rates are given by

$$\gamma_x + \gamma_y \equiv \gamma_{XX}, \quad \gamma'_x = \gamma'_y \equiv \gamma_X\,. \tag{3.26}$$

Since the biexciton decays twice as fast according to Eq. (3.6), if we assume identical group velocities we have that $\gamma_X = \gamma_{XX}/2$. In the rest of the article, we assume this relation between the spontaneous emission rates.

The difference in the phase of the transition dipoles for biexciton and exciton decays, Φ and Φ' respectively, satisfies Eq. (3.12). Moreover as the optical wavelengths of the photons emitted from biexciton and the exciton decay channels are comparable, we can approximate the phase differences to be equal, i.e. $\Phi = \Phi'$. Under these assumptions, the total probability of detecting the first photon at time $t = t_{XX}$ is

$$P(t = t_{XX}) = (\gamma_x + \gamma_y)e^{-(\gamma_x+\gamma_y)t_{XX}/\hbar} = 2\gamma_X e^{-2\gamma_X t_{XX}/\hbar}\,. \tag{3.27}$$

We can thus calculate the path-dependent, two-photon emission probabilities to be

$$\begin{aligned} P_{AA} &= \frac{\gamma_X}{4} e^{-\gamma_X\tau/\hbar}\left(1 + \cos\left(S\tau + 2\Phi\right)\right) \\ P_{BB} &= \frac{\gamma_X}{4} e^{-\gamma_X\tau/\hbar}\left(1 + \cos\left(S\tau - 2\Phi\right)\right) \\ P_{AB} = P_{BA} &= \frac{\gamma_X}{4} e^{-\gamma_X\tau/\hbar}\left(1 + \cos\left(S\tau\right)\right)\,. \end{aligned} \tag{3.28}$$

A QD with $S = 0$ that is perfectly chiral coupled to the waveguide, i.e., $\Phi = \Phi' = \pi/2$, results in $P_{AA} = P_{BB} = 0$. In this case we thus have the ideal entangled state $(|AB\rangle + |BA\rangle)/\sqrt{2}$, where the emission direction of the two photons is perfectly anticorrelated, as shown with blue and orange lines in Fig. 3.2. Note that, for $S = 0$, our model can only accurately represent the perfect chiral coupling case and will lead to erroneous conclusions if $\Phi \neq \pi/2$ since this leads to $\Gamma \neq 0$. For the general case of $S > 0$, we can calculate the resulting entangled two-photon state by conditioning the solution in Eq. (3.21) on the detection of a photon at time $t = t_{XX}$. For perfect chiral coupling the state is

$$|\psi(\tau)\rangle_{\Phi=\pi/2} = \frac{1}{2}(\cos\left(\frac{S\tau}{2}\right)(|AB\rangle + |BA\rangle) + i\sin\left(\frac{S\tau}{2}\right)(|AA\rangle + |BB\rangle))\,, \tag{3.29}$$

To understand the entanglement in this state we rewrite it as

$$|\psi(\tau)\rangle_{\Phi=\pi/2} = \frac{1}{2}(|A\rangle|\xi\rangle + |B\rangle|\xi'\rangle)\,, \tag{3.30}$$

which is in fact a maximally entangled state, with $|\xi\rangle = \cos(S\tau/2)|B\rangle + i\sin(S\tau/2)|A\rangle$ and $|\xi'\rangle = \cos(S\tau/2)|A\rangle + i\sin(S\tau/2)|B\rangle$. For perfect chirality the entanglement is thus maximal regardless of the detection time, although the specific entangled state varies with the emission time, resulting in a time varying detection pattern in Fig. 3.2. In contrast, if the waveguide interaction is not chiral ($\Phi = 0, \pi$) the state is given by

$$\begin{aligned} |\psi(\tau)\rangle_{\Phi=0,\pi} &= \frac{1}{2}\left(|AB\rangle + |BA\rangle + |AA\rangle + |BB\rangle\right) \\ &= \frac{1}{2}\left(|A\rangle + |B\rangle\right)_X\left(|A\rangle + |B\rangle\right)_{XX}\,, \end{aligned} \tag{3.31}$$

which is a separable state. As a consequence all detection patterns of two photons are equally probable. In real experimental settings, the directional (chiral) coupling could lie in between these two extreme cases depending on the local electric field at the location of the QD within the waveguide. This imperfect chirality will lower the entanglement quality of the source, which is quantified in the next section.

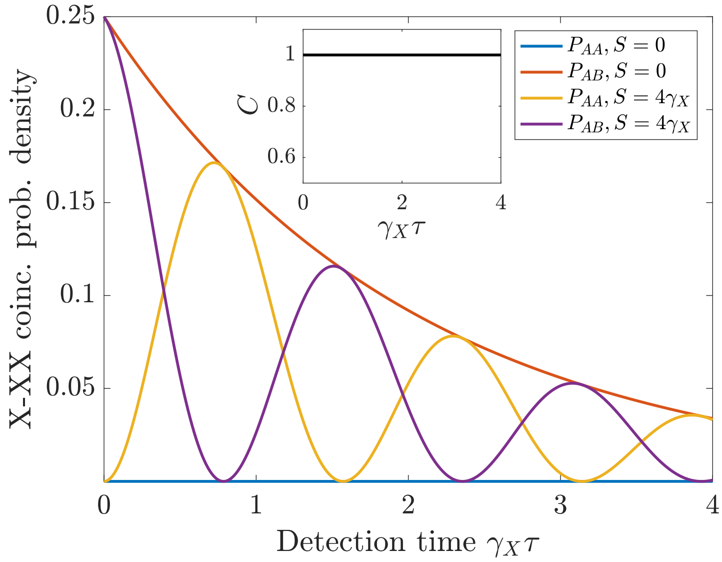


Figure 3.2: Time correlations P_{AA} and P_{AB} as a function of the difference in the emission time τ. The blue and orange lines have been calculated with perfect symmetry between the exciton levels ($S = 0$) while the yellow and purple lines have been obtained for $S = 4\gamma_X$. The waveguide coupling is perfectly chiral ($\Phi = \pi/2$) in all cases. *Inset.* Concurrence C of the state as a function of the difference in emission times τ. The concurrence remains unity at all times for any value of S. This shows that the state is maximally entangled independently of the time τ, as also shown in Eq. (3.29).

3.3 Results

As we have seen in the previous section, the emitted two-photon entangled state depends on the time difference τ between the biexciton and exciton emission times. We thus expect that any uncertainty in the emission times will affect the entanglement quality of the state. Moreover, imperfect chirality of the waveguide reduces the directionality of emission, thereby leading to non-perfect conversion into path encoding of the entangled state. In this section, we quantify the effect of imperfections on the entanglement quality of the state.

To this end, we employ the concurrence C as the entanglement measure to characterise the quality of the state. The concurrence of any quantum state with a density matrix ρ is given by (Fan et al., 2003)

$$C(\rho) = \max\{0, \lambda_1 - \lambda_2 - \lambda_3 - \lambda_4\}\,, \tag{3.32}$$

where $\{\lambda_i\}$ are the square root of the eigenvalues of $\rho\tilde{\rho}$ in descending order and $\tilde{\rho} = (\hat{\sigma}_y \otimes \hat{\sigma}_y)\rho^*(\hat{\sigma}_y \otimes \hat{\sigma}_y)$. We calculate the density matrix ρ that represents the path-encoded state obtained from the biexciton cascade to be

$$\rho(\tau) = \sum_{\substack{n,n' \\ m,m'}} \psi_{n,m}(\tau)\psi^*_{n',m'}(\tau)\,|n,m\rangle\,\langle n',m'|\;. \tag{3.33}$$

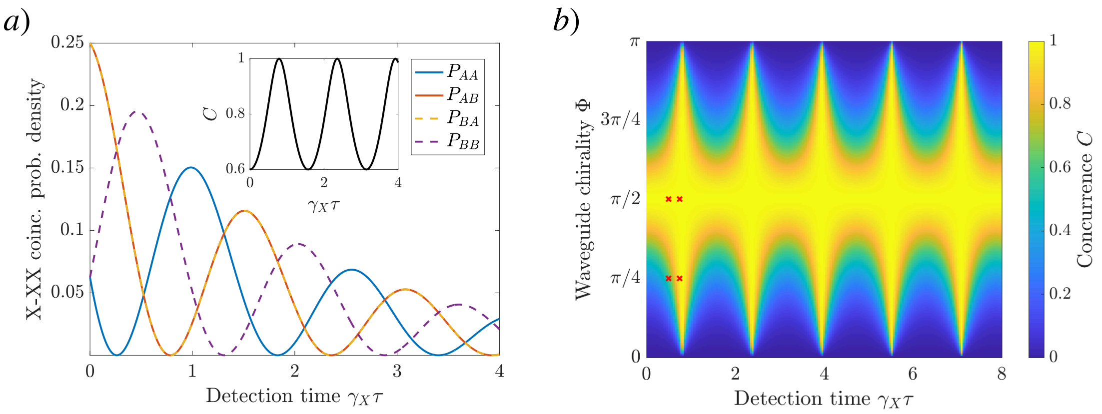


Figure 3.3: a) Time correlations P_{AA}, P_{AB}, P_{BA}, P_{BB} as a function of the difference in the emission time τ with a FSS of $S = 4\gamma_X$ and waveguide chirality of $\Phi = \pi/3$. We observe that P_{AA} and P_{BB} are out of phase with each other. This may seem surprising, since the two directions are naively the same, but occurs due to an interplay between the imperfect chirality and the sign of the FSS (see text). This effect was experimentally observed in Østfeldt et al. (2022). *Inset.* Concurrence C of the state as a function of the difference in emission times τ. The concurrence oscillates between 0 and 1, as the state evolves. b) Colour map of the concurrence C of the state as a function of the difference in phase Φ and the difference in emission times τ. The concurrence oscillates in time for a given chirality, with the exception of perfect chirality ($\Phi = \pi/2$ which gives $C = 1$) and non-chiral waveguide coupling ($\Phi = 0, \pi$ which gives $C = 0$). The red "×"-markers indicate the points investigated in Figure 3.4(a).

By calculating the resulting eigenvalues $\{\lambda_i\}$, we obtain the concurrence using Eq. (3.32)

$$C(\tau) = \frac{2}{N}|\psi_{AA}(\tau)\psi_{BB}(\tau) - \psi_{AB}(\tau)\psi_{BA}(\tau)|\,. \tag{3.34}$$

Inserting the wavefunctions from Eq. (3.21) and approximating $\gamma_x = \gamma_y$ as discussed earlier (cf. Eq. (3.26)), the dependence of C on the chiral phase Φ and the time delay between biexciton and exciton emissions τ is found to be

$$C(\Phi,\tau) = \frac{\sin^2(\Phi)}{1+\cos(S\tau)\cos^2(\Phi)}\,. \tag{3.35}$$

We obtain perfect concurrence $C = 1$ when the waveguide is perfectly chiral ($\Phi = \pi/2$) as discussed above. Furthermore, if the waveguide is completely non-chiral ($\Phi = 0, \pi$) the concurrence vanishes $C = 0$, agreeing with the separable state obtained in Eq. (3.31). In the following subsections we will independently analyse the effect of each of the imperfections in more detail.

3.3.1 Fine-structure splitting

In this subsection, we analyse the effect of the FSS on the entanglement quality of the path-entangled state. Non-zero FSS leads to a spin-flip between the exciton levels

($|X_{\pm}\rangle$), and it is therefore convenient to describe the decay in the linear polarisation basis with x- and y-polarized states, $|X_x\rangle$ and $|X_y\rangle$ respectively (c.f. Fig. 5.2(b)). In this basis, the states are decoupled and the FSS induced spin-flip frequency S corresponds to an energy splitting between the exciton levels. The splitting makes the emitted photons distinguishable in energy, and crucially their frequencies are correlated with their polarisations. This leads to "which-way" information about the polarisation state, which means reduction in the degree of entanglement. To overcome this issue Fognini et al. (2018) has proposed using electro-optical modulators that rotate the polarisation of the biexciton and exciton photons separately to effectively erase the information gained from the splitting in the polarisation-encoded state. A phase modulator could similarly be applied to improve path-entangled states. Alternatively, narrow spectral filtering in between the two frequency components of either the exciton or biexciton emission can be implemented to erase the "which-path" information, however, at the expense of significantly reducing the entanglement generation rate (Akopian et al., 2006). Another approach is to implement QDs with improved symmetry in order to obtain a smaller splitting S (Huo et al., 2013).

The reference situation corresponds to an ideal system without fine structure splitting and perfect directional (chiral) coupling ($S = 0$ and $\Phi = \pi/2$). This situation is easily understood from the level structure in Fig. 5.2(a), where emission occurs with two oppositely polarized circular dipoles (σ_- and σ_+). With perfect chiral coupling these decay in opposite directions creating that maximally entangled state $(|AB\rangle + |BA\rangle)/\sqrt{2}$. As a consequence, the probability of detecting both photons on the same side of the waveguide vanishes (blue line in Fig. 3.2). The probability of detecting one photon at each of the opposite ends of the waveguide decays exponentially with the exciton spontaneous emission rate $(\gamma'_x+\gamma'_y)/2$ (orange line in Fig. 3.2) as expected from the lifetime of the exciton states.

We now consider a scenario where the FSS creates an asymmetry between the exciton levels ($S \neq 0$), while the chiral coupling is still ideal ($\Phi = \pi/2$). This generates an oscillation between two maximally entangled states as discussed below Eq. (3.30). The corresponding probabilities of the various detection patterns is shown with the yellow and purple lines in Fig. 3.2. The amplitude of oscillations decays exponentially with the time constant set by the exciton spontaneous emission rate. As discussed in the previous section, although the emitted state changes over time, it remains maximally entangled, i.e., $C(\tau \geq 0) = 1$, and it is a superposition of standard Bell states.

3.3.2 Imperfect chirality

We now analyse the joint effect of both imperfect chirality ($\Phi \neq \pi/2$) and non-zero FSS ($S \neq 0$). An example of the detection probability for this situation is shown in Fig. 3.3(a). Curiously, the probabilities P_{AA} and P_{BB} are out of phase, meaning that with a given time delay there is a difference in the probabilities of detecting two photons at the two ends of the waveguide. This effect happens due to an interplay of the imperfect chirality and the FSS. A decay from the biexciton state and subsequent detection of the photon at one end creates a coherent superposition between the two exciton states $|X_x\rangle$ and $|X_y\rangle$ with a phase $\mp\Phi$ depending on where the photon was detected. The subsequent dynamics induced by the FSS S may then evolve the state towards or away from the relative phase $\pm\Phi$, which gives the maximal emission in the same direction.

With non-perfect chirality, the concurrence C of the path-entangled, bi-photon state emitted by the biexciton cascade is reduced since the imperfect chirality limits the directional coupling of the QD emission. The dependence of $C(\tau)$ on Φ is shown in Fig. 3.3(b). We observe that C is independent of τ only if $\Phi = n\pi/2$, where n is a non-zero integer. If n is even, $C(\tau \geq 0) = 0$ and corresponds to the completely non-chiral case. If n is odd, we reproduce the results of the perfect chiral case that results in a maximally entangled state with $C(\tau \geq 0) = 1$ as discussed in the previous subsection. For partial chirality $\Phi \neq \pi/2$, the FSS induces oscillations between non-maximally entangled states and C oscillates as a function of the detection time τ. In general, C is below unity except for $S\tau = \pi$, where the concurrence is unity for all $\Phi \neq 0, \pi$.

3.3.3 Timing jitter

In this subsection we analyse the effect of uncertainty in the timing of photodetection events on the entanglement quality. We model the uncertainty in detection time by averaging the density matrix (3.33) elements $\rho_{n,n',m,m'}$ with a Gaussian probability distribution with standard deviation σ

$$\bar{\rho}_{n,n',m,m'}(\tau) = \int_0^\infty d\tau' \exp\left[-\frac{(\tau'-\tau)^2}{2\sigma^2}\right] \psi_{n,m}(\tau')\psi^*_{n',m'}(\tau') \,. \tag{3.36}$$

The time-averaged density matrix $\bar{\rho}(\tau)$ is then given by

$$\bar{\rho}(\tau) = \frac{1}{\bar{N}(\tau)} \begin{pmatrix} \bar{\rho}_{AAAA}(\tau) & \bar{\rho}_{AAAB}(\tau) & \dots & \bar{\rho}_{AABB}(\tau) \\ \bar{\rho}_{ABAA}(\tau) & \ddots & & \vdots \\ \vdots & & \ddots & \vdots \\ \bar{\rho}_{BBAA}(\tau) & \dots & \dots & \bar{\rho}_{BBBB}(\tau) \end{pmatrix} , \tag{3.37}$$

where $\bar{N} = \int_{-\infty}^{\infty} d\tau' \exp[-(\tau'-\tau)^2/(2\sigma^2)]N$ is a normalisation constant equal to the probability density of the detection time and N is given by Eq. (3.25). From this density matrix we can then calculate the concurrence C.

Figure 3.4(a) shows the dependence of the concurrence C on the detection timing jitter σ at different combinations of chirality and time delay. As seen in the figure the concurrence drops when the uncertainty in detection time becomes comparable to the oscillation period $1/S$. This highlights the importance of keeping track of the time dependence for the quality of the final path-entangled state. Unlike the

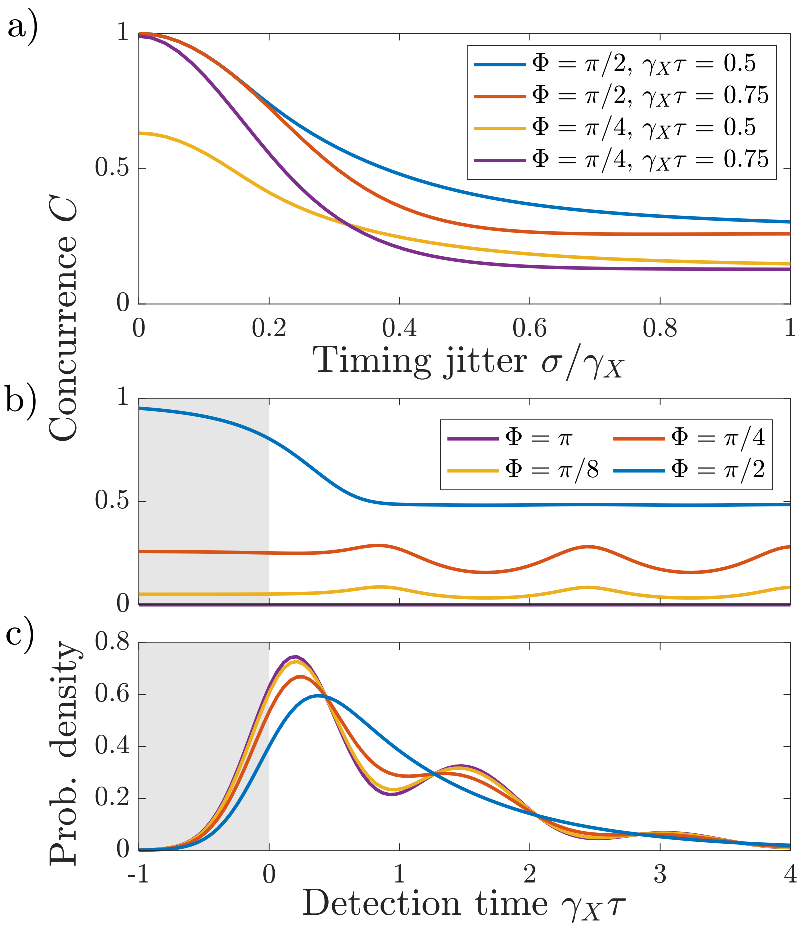


Figure 3.4: a) Concurrence C of the state as a function of the detection timing jitter, quantified by the Gaussian RMS width σ, for several values of chirality Φ and time difference τ (the selected values are marked with red $\times$-symbols in Fig. 3.3(b)). b) Concurrence C of the state for different degree of chirality, quantified by the phase Φ, with a timing jitter of $\sigma = 0.3/\gamma_X$. The concurrence can be larger at negative than positive time intervals (grey shaded region) since such events effectively have less timing uncertainty than those with positive time intervals (see text). c) Corresponding probability density $\bar{N}$ of the detection time for the situation analysed in (b). Note that the probability density quickly approaches zero for $\tau < 0$ (grey) in contrast to the increase in concurrence. Throughout the figure we assume a non-zero FSS of $S = 4\gamma_X$.

jitter-free case, even systems with perfect chirality ($\Phi = \pi/2$) exhibit $C < 1$ for non-zero values of σ since we do not know precisely which state we have. The asymptote of C with increasing time jitter is observed to depend only on the phase Φ, i.e., when the time jitter is comparable to or larger than the spread in emission time; the precise time of the detection is not important. Figure 3.4(b) shows the time evolution of C for a fixed timing jitter $\sigma = 0.3/\gamma_X$ for different values of the chiral phase and $S = 4\gamma_X$. Note that a peculiar effect occurs for $\Phi = \pi/2$ (Fig. 3.4(b)), where we observe that C increases at negative time delays (grey shaded region). Since the emission of the exciton always occurs after the biexciton emission ($t_X - t_{XX} = \tau > 0$), negative detection intervals ($\tau < 0$) correspond to the case where the emission of the photon must have occurred close to $\tau = 0$, i.e. with minimal time delay, but was measured to be at a negative value due to the time jitter. Therefore the uncertainty in the emission time, which is otherwise given by the detection time jitter, is effectively reduced for negative detection times, leading to a higher concurrence. The probability of measuring the state at negative time intervals, however, decays very rapidly as τ decreases, as shown in Fig. 3.4(c). The larger concurrence at small positive time delays ($0 < \tau \lesssim \sigma$) compared to later times can be understood with similar arguments. On the other hand for $\Phi = \pi/4$ and $\Phi = \pi/8$ the fidelity in the absence of time jitter is lower around $\tau = 0$ than at later times, c.f. Fig. 3.3(b). As a consequence the peak concurrence still occurs around $S\tau = \pi$. The probability density in Fig. 3.4(c) decays with the decay rate γ_X of the exciton states. On top of this it oscillates with increasing amplitude as the system becomes less chiral ($\Phi \to 0$). The reason is that the polarisation of waveguide modes becomes linear as the system loses chirality. After the decay of the biexciton, the polarisation of the exciton state rotates due to the FSS S and may thus be more or less aligned with the waveguide polarisation. In contrast, for the chiral case the waveguide polarisation is circular and the rotation of the polarisation does not affect the decay rate.

3.3.4 Asymmetric exciton decay

In the experiments presented in Østfeldt et al. (2022), the decay rates of the x and y-polarized exciton levels were nearly identical (i.e. $\gamma_x \approx \gamma_y$). However, in general these two decay rates may differ depending on the position of the QD in the waveguide, with the asymmetry more dominant at locations with a low degree of directional emission, i.e., far from perfect chirality. In this subsection we analyse how this asymmetry can affect the quality of entanglement.

Figure 3.5(a,b) shows the impact of asymmetry $\epsilon \equiv (\gamma_x - \gamma_y)(\gamma_x + \gamma_y)$ on the concurrence for the case of $\epsilon = -0.4$. As the decay rates of the x- and the y-polarized exciton levels are different, one can gain "which path" information about the photon decay from the photodetection time, i.e. the highest decay rate would result in increased likelihood of early detection of photon, and vice versa. This extra information about the emission process reduces the entanglement. Furthermore, the

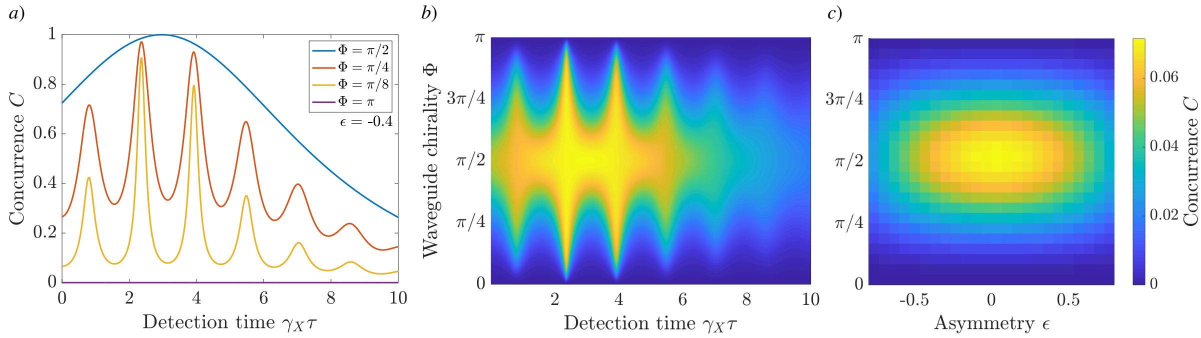


Figure 3.5: a) Concurrence C of the state as a function of the time delay τ at different degrees of the chirality, quantified by Φ. The asymmetry between the exciton decay rates is described by the parameter $\epsilon = (\gamma_x - \gamma_y)/(\gamma_x + \gamma_y)$ and fixed to be $\epsilon = -0.4$. The oscillations in the concurrence due to the FSS $S = 4\gamma_X$ are modulated by the difference in exciton decay rates. b) Colour map of the concurrence of the state as a function of the difference in phase Φ and the time τ for $\epsilon = -0.4$. The concurrence oscillates in time due to the FSS S, and reaches a maximum for a non-zero time τ. This optimal difference in emission time is reached when the difference in populations of the exciton states arising from a difference in biexciton decay rates is cancelled by the faster decay of the most likely state. c) Colour map of the concurrence $\bar{C}$ averaged over all emission times τ as a function of the difference in phase Φ and the asymmetry parameter ϵ with $S = 4\gamma_x$ and a time jitter of $\sigma = 3/\gamma_X$. We observe that the concurrence is optimal for perfectly symmetric exciton decays, as expected.

difference in decay rates of the biexciton state creates a difference in populations of the $|X_x\rangle$ and $|X_y\rangle$ states. However, if the difference in the emission time is comparable to the difference in decay rates, the 'which path' information arising from the asymmetric decay rates is erased and the entanglement is recovered. This interplay between the difference in emission times and the asymmetry ϵ leads to an optimal time delay τ that maximizes the concurrence as observed in Fig. 3.5(a,b). In addition to this optimality, we still observe that C oscillates with emission time delay due to the non-zero S as discussed in Sec. III.A.

For a systematic study of the effect of asymmetry, we calculate the average concurrence $\bar{C}$ over all τ detection times, defined as

$$\bar{C} = \int_{-\infty}^{\infty} P(\tau)C(\tau)d\tau\,, \tag{3.38}$$

where $P(\tau)$ is the corresponding probability density of the state at time τ. The dependence of $\bar{C}$ on the asymmetry parameter ϵ and the phase difference Φ is shown in Fig. 3.5(c), which highlights that $\bar{C}$ is maximized for symmetric decay of the exciton dipoles, i.e. $\epsilon = 0$.

3.4 Conclusion

We have provided an in-depth analysis of the entanglement properties of a QD biexciton cascade embedded in a chiral nanophotonic waveguide, as experimentally realised in Østfeldt et al. (2022). We have calculated how the biexciton cascade can deterministically prepare a path-encoded state mediated by the chiral-coupling of the waveguide. The entanglement of the state is, however, affected by errors unavoidably present in the experimental implementation of the system. In particular, we have shown how the time dependence of the state induced by the FSS plays a crucial role in determining the generated entanglement. The amount of path-entanglement generated by the biexciton cascade can strongly depend on the emission time, while the presence of detection time jitter reduces the concurrence of the state. Finally, imperfect directional-coupling in the waveguide reduce the concurrence of the path-encoded entangled state as well. Our work quantifies the role of such imperfections and lay out a route to a deterministic source of path-encoded entangled photons of high entanglement quality. We hope our work will motivate further experimental improvements of this novel entanglement source.

Chapter 4

New key-rate lower bounds for DIQKD implementations with single-photon sources

This chapter is based on the preprint González-Ruiz et al. (2022b)[1]. We investigate the proposal for performing fully photonic DIQKD already introduced in Chapter 1, based on single-photon sources and heralding measurements at a central station placed between the two parties. We derive conditions to attain non-zero secret-key rates in terms of the the photon efficiency, indistinguishability and the second order autocorrelation function of the single-photon sources. Exploiting new results on the security bound of such protocols allows us to reduce the requirements on the physical parameters of the setup. Our analysis shows that in the considered schemes, key rates of several hundreds of secret bits per second are within reach at distances of several tens of kilometers.

4.1 Introduction

The use of quantum mechanics to establish secure communication between two parties, Alice and Bob, is the essence of Quantum Key Distribution (QKD) where the parties use a quantum channel to establish a secret key (Bennett et al., 1984; Ekert, 1991). Experimental demonstrations of QKD protocols have been successfully carried out in a number of setups, see for instance Scarani et al. (2009), and QKD devices are now commercially available. The security of QKD protocols relies on several assumptions, in particular:

1. Quantum mechanics is a valid theory,

[1]The Ph.D. student participated in the discussions that shaped both the initial version of the project and the following directions it took. She carried out all the analysis and relevant optimisations together with JRD, who contributed equally as much. She contributed to writing the Introduction and Conclusion and was responsible for the Experimental setup section, together with the first two appendices of the paper.

2. Alice and Bob trust their device and therefore assume that they are performing the operations described by the QKD protocol.

The aim of Device Independent Quantum Key Distribution (DIQKD) (Acín et al., 2007) is to remove the last assumption, which can be a source of various possible hacking attacks (Lydersen et al., 2010). The security of a DIQKD protocol depends on the statistics obtained by the parties without requiring any physical model of the measurements or of the state used in the protocol. The security of such protocols has been successfully proven even when allowing an eavesdropper, Eve, to perform general attacks, see e.g. Arnon-Friedman et al. (2019).

A DIQKD protocol is an entanglement based protocol where Alice and Bob possess two measurement apparatus, which are considered to be black boxes, on which one can define *settings* and obtain *outcomes*. The security of the protocol relies on the violation of a Bell inequality (Acín et al., 2007). Intuitively, for some Bell inequalities, e.g. the Clauser-Horne-Shimony-Holt (CHSH) inequality (Clauser et al., 1969), if the two parties observe a maximal violation, they share a maximally entangled two-qubit state (Mayers et al., 2004; Kaniewski, 2016) and thus cannot be correlated with a third party. In practice, however, the maximum violation of such an inequality can never be achieved because of the inevitable noise present in experiments. Reduced violations introduce the possibility that the two parties are correlated with Eve, so that when the Bell violation becomes smaller than a critical value, no secret key can be established. In fact, the noise requirements needed to produce a secret key happen to be very challenging to meet in practice.

The implementation of standard entanglement-based QKD is based on the distribution of entangled photons. However, the high requirements with respect to noise make direct transmission of an entangled pair of photons undesirable for DIQKD. Indeed the unavoidable transmission losses between the two parties prevent such scheme from working unless losses are very small, that is, the users are very close. To circumvent transmission losses one can use a heralding scheme, where entanglement is generated between the local stations conditioned on the detection of photons at a central heralding station (CHS), which performs a Bell state measurement (BSM) on photonic fields entangled with each of the two stations. This gives the major advantage since successful entanglement is heralded, photon loss does not influence the quality of the entangled states; it lowers the success probability but the protocol remains secure.

The first experimental demonstrations of DIQKD have been performed very recently using heralding schemes (Nadlinger et al., 2022; Zhang et al., 2022). In those experiments the state at the local stations are encoded in material qubits, in particular Nadlinger et al. (2022) uses two trapped ions and Zhang et al. (2022) uses two trapped rubidium atoms. The advantage of such encoding lies in the very high efficiency of the measurement of the matter degree of freedom, allowing for a sufficiently high violation of the CHSH inequality to perform DIQKD. On the other hand, such encodings into material qubits typically require rather advanced setups and often suffer from low repetition rates, making the application of such setups less desirable for practical applications. In fact, the experiment of Nadlinger et al. (2022) was able to report a positive rate between users distant 2 meters, while the experiment of Zhang et al. (2022) demonstrated a Bell violation between users distant 400 meters that was large enough in principle to establish a secure key, although the number of runs in the experiment were not enough to achieve this.

Photonic experiments can in principle alleviate these problems because they have a higher repetition rate, but suffer from limited measurement efficiency. Heralding schemes based on photonic implementations using a spontaneous parametric down conversion (SPDC) source and a qubit amplifier (Gisin et al., 2010) have been proposed as a means to perform DIQKD, but suffer from an unfavorable scaling with distance see e.g Appendix B of Kołodyński et al. (2020). On the other hand, single-photon sources, and in particular those based on InGaAs quantum-dot, are able to generate on-demand single photons with high indistinguishability and purity, up to 96% and 99.4% respectively (Tomm et al., 2021; Uppu et al., 2020). These single-photon sources are currently being developed towards fully integrated devices, and are thus suitable candidates for scalability of DIQKD implementations in the near future. Recently, heralding schemes for DIQKD based on such single-photon sources (Kołodyński et al., 2020) have been developed and these were shown to have a more promising scaling with distance, although requiring high detection efficiencies.

The security of the experimental protocols presented above were based on the violation of the CHSH inequality. Such security proofs of DIQKD have been extended to generalized CHSH inequalities (Sekatski et al., 2021; Woodhead et al., 2021). The choice of the correct Bell inequality is crucial, as different inequalities can lead to higher robustness of the protocol with respect to noise[2]. Recently, a breakthrough regarding the choice of inequality was achieved in Brown et al. (2021), where the authors derived a method for guaranteeing the security of protocols based on all the observed statistics. This method is equivalent to the optimization of the security of the protocol with respect to all possible Bell inequalities. This approach thus allows for improving the noise robustness of DIQKD protocols.

In this work, we improve the previous derived experimental requirements for the purely photonic implementation of DIQKD with single-photon sources proposed in Kołodyński et al. (2020), and further analyzed in González-Ruiz et al. (2022a) (see Chapter 1). The main contribution of this work is to study the experimental requirements for photonic DIQKD experiments with single-photon sources. In particular we focus on single-photon emission from quantum dots. In Section 4.2, we present the proposed setup and characterize the main parameters that limit the experimental implementation. In Section 4.3, we briefly review the security of the protocol and the method used in Brown et al. (2021). In Section 4.4, we analyze the robustness of the protocol in a realistic scenario where we consider limited local efficiency, indistinguishability and purity of the single-photon source. Here, we also perform a finite statistics analysis of our results and study the security of the protocol with

[2] Appendix **??** shows the equivalence between CHSH and Eberhard's inequalities when one assigns a determined outcome to inconclusive events.

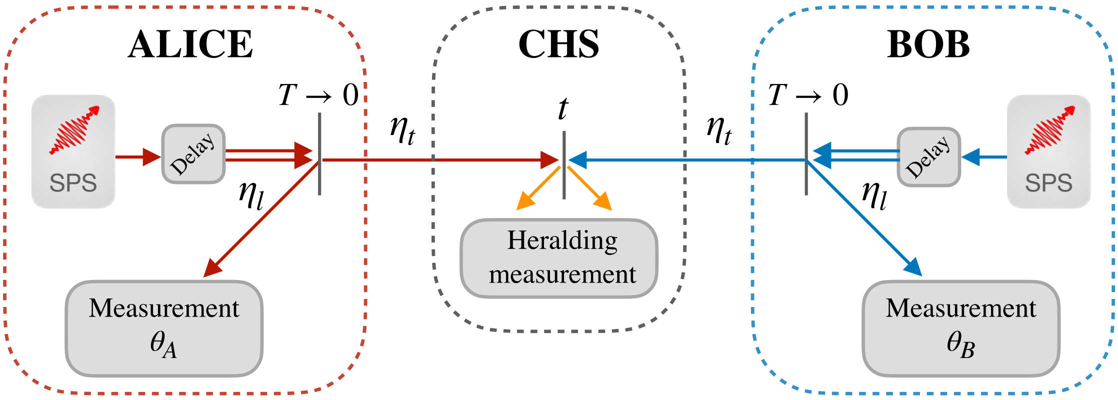


Figure 4.1: Heralded set-up introduced in Ref. (Kołodyński et al., 2020). Alice and Bob each possess a single-photon source, which by means of an optical delay circuit provides two simultaneous photons with orthogonal polarizations. One of them is transmitted from each lab through a low transmittance beam splitter ($T \to 0$) with efficiency η_t to a central heralded station (CHS) that performs a Bell state measurement. The entanglement of the the polarization state of Alice and Bob's remaining photons after the CHS measurement can be tuned depending on the transmittance t of the beam splitter at the CHS. The basis choice of the local measurements is defined by the angle θ_A (θ_B) of a certain combination of half-wave and quarter-wave plates (González-Ruiz et al., 2022a). The total local efficiency at Alice and Bob's stations is denoted by η_l.

respect to time and distance.

4.2 Experimental setup

In this work, we consider the set-up that is pictorially presented in Fig. 4.1, where Alice and Bob generate two single-photons, each with orthogonal polarization, by means of a single-photon source and an optical delay line (González-Ruiz et al., 2022a). The photons are sent towards a low-transmittance ($T \to 0$) beam-splitter such that, with very good approximation, the detection of two photons at the (CHS) signals that at each user's local station, one of the photons was sent to the CHS and the other is kept. Thus, the outcome of the measurement at the CHS heralds the successful generation of the desired entangled polarization state between the remaining photons at Alice and Bob's stations. In this way the expected low transmission efficiency between Alice and Bob due to their spatial separation does not open the detection loophole; since photons at the local stations have propagated a short distance, they have only suffered limited loss, and are thus detected with very high probability.

The heralding signal at the CHS creates an entangled state in polarization by performing a Bell state measurement (Kwiat et al., 1998). The entangled state is proportional to

$$|\psi\rangle \propto |{+}{-}\rangle - \frac{t}{1-t}|{-}{+}\rangle \,, \tag{4.1}$$

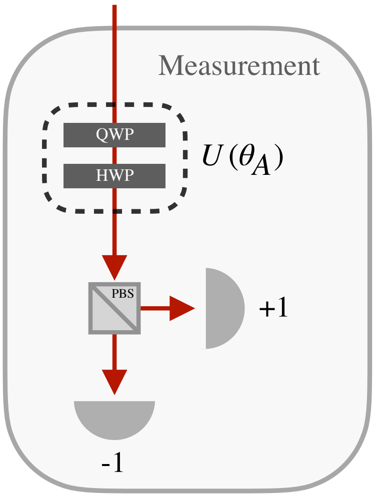


Figure 4.2: Measurement set-up in Alice's station. The half-wave plate (HWP) and quarter-wave plate (QWP) set the basis choice by fixing the relative angle θ_A. A polarising beam splitter (PBS) directs photons with orthogonal polarisation to two detectors, whose outcomes are identified as ± 1 respectively.

where $|\pm\rangle = \frac{1}{\sqrt{2}}(|H\rangle \pm |V\rangle)$, with $|H\rangle$ and $|V\rangle$ the states with horizontal and vertical polarization respectively and t is the transmittance of the beam splitter at the CHS. Note that by varying t, the state shared by Alice and Bob can vary from a Bell state to a non-maximally entangled state arbitrary close to a separable state. If $t = 0.5$, the state corresponds to the Bell state $|\psi^-\rangle = \frac{1}{\sqrt{2}}(|HV\rangle - |VH\rangle)$ and we recover the set-up and results from González-Ruiz et al. (2022a), while if $t = 0$ or 1 no entanglement is created. Being able to optimize the degree of entanglement in non-maximally entangled states is a very useful feature, as it can reduce the required efficiency for the violation of Bell's inequality (Eberhard, 1993). Crucially, with the presented scheme the state shared between the two parties does not depend on the channel transmission efficiency η_t, and therefore it allows for extending the communication distance without compromising the violation of a Bell inequality and hence the security of the protocol. The local efficiency η_l between the source and measurement at Alice and Bob's stations remains, however, the main challenge since this measurement is not heralded. Furthermore, due to the different experimental errors (limited indistinguishability, purity and non number-resolving detectors) the state is not a pure state.

The local measurements of Alice and Bob are performed in the polarization basis. Before detecting the photons, they transform the state according to a linear transformation $U(\theta_A) \otimes U(\theta_B)$ by means of a set of half-wave plates and quarter-wave plates (see Fig. 4.2). Once the state has been successfully rotated to the desired basis the photons are directed to a polarising beam splitter that sends them to two different detectors. Thereby they can measure the state in any desired basis. Note that one can find a plane in the Bloch sphere such that only the relative angle between the half-wave and quarter-wave plates (which we define as θ_A and θ_B for

$p(a=\pm1,b=\pm1\|x,y)$	$p(a=\pm1,b=\emptyset\|x,y)$	$p(a=\emptyset,b=\pm1\|x,y)$	$p(a=\emptyset,b=\emptyset\|x,y)$
p_{2110}	$p_{2200,SD}$	$p_{2020,SD}$	p_{2002}
	p_{2101}	p_{2011}	$p_{2200,DD}$
			$p_{2020,DD}$
p_{2111}	p_{2102}	p_{2012}	p_{2003}
$p_{2210,SD}$	$p_{2201,SD}$	$p_{2021,SD}$	$p_{2201,DD}$
$p_{2120,SD}$	$p_{2120,DD}$	$p_{2210,DD}$	$p_{2021,DD}$
	$p_{2300,SD}$	$p_{2030,SD}$	$p_{2300,DD}$
			$p_{2030,DD}$

Table 4.1: Probability contributions to the total probability of detection $p(a_i,b_i|x_i,y_i)$, where the outcome $a,b=\emptyset$ indicates that no photon was detected and $a=\pm1$ ($b=\pm1$) is a classical binary output. The four sub-indexes indicate the number of photons detected at the CHS, Alice's and Bob's stations and that were undetected, respectively. The probability contributions are divided between those involving four photons (above the middle line) or five (below the middle line), where the fifth one is generated due to imperfect purity of the single-photon source ($g^{(2)}\neq 0$). If more than one photon is detected at the local stations we specify whether they were detected at the same (SD) or different (DD) detectors. As we do not consider number-resolving detectors, in the first case Alice and Bob identify these events as correct. However, if photons click in different detectors they recognise that an error occurred and thus assign the outcome to be $\emptyset$.

Alice's and Bob's measurement, respectively) is the degree of freedom to optimise, which simplifies greatly the computation later on.

We consider non photon-number resolving detectors, this is, they only measure the arrival of photons. Thus the detectors are defined by the Positive-Operator-Valued-Measure (POVM) operators $\{\hat{M}_{j,A}\}$ ($\{\hat{M}_{j,B}\}$) with $j\in\{0,1\}$, where $\sum_j \hat{M}_{j,A} = \mathbb{I}$ ($\sum_j \hat{M}_{j,B}=\mathbb{I}$) and

$$\hat{M}_{0,A} = |\emptyset\rangle\langle\emptyset|_A\,,\quad \hat{M}_{1,A} = \mathbb{I} - |\emptyset\rangle\langle\emptyset|_A\,, \tag{4.2}$$

and similarly for Bob. The state $|\emptyset\rangle$ is the vacuum state, and the subscripts 1 and 0 define the different outcomes that can be obtained. Depending on which detector clicked, they obtain a classical outcome ±1. If no detector clicked ($\emptyset$), they assign the outcome to $+1$. Since the detectors are not number-resolving, this induces errors for certain detection combinations. For instance, the two photons generated by Alice may be reflected at the first beam splitter, while both of Bob's photons are transmitted to the CHS giving the correct detection pattern.

We denote by $\hat{\rho}$ the state of Alice and Bob after an heralding event at the CHS. The probability of detection $p(a_i,b_j|x_d,y_q)$ has classical inputs $\{x_d,y_q\}$ and classical outputs $\{a_i,b_j\}$, where $x_d=\theta_{A,d}$ ($y_q=\theta_{B,q}$) represents Alice (Bob) inputs. Thus the probability of detection is given by

$$p(a_i,b_j|x_d,y_q) = \mathrm{Tr}\left\{\left(\hat{M}_{i,A}\otimes\hat{M}_{j,B}\right)\hat{\rho}'\right\}, \tag{4.3}$$

where $\hat{\rho}' = U(\theta_{A,d})\otimes U(\theta_{B,q})\hat{\rho}U^\dagger(\theta_{A,d})\otimes U^\dagger(\theta_{B,q})$. Each of these probability contributions includes the probability of all the events that lead to the acceptance at the CHS and not only the ideal scenario (see Table 4.1). Following González-Ruiz et al. (2022a) we label each of these probability terms as p_{klmn}, where the indexes indicate the number of photons detected at the CHS (k), Alice's and Bob's stations (l and m) and undetected (n), respectively.

Another source of errors is the indistinguishability of two photons. This is directly related to the Hong-Ou-Mandel (HOM) visibility V_{HOM} (González-Ruiz et al., 2022a): the higher the visibility, the more indistinguishable the photons are. The precise nature of the indistinguishability, on the other hand, depends on the decoherence mechanisms of the single-photon source. Since in this work we consider implementations using single-photon sources based on quantum dots, we focus on fast (pure) dephasing with rate γ_d, e.g. due to phonon interaction with the quantum dot, as this is the biggest source of noise for quantum dots at the relevant timescale (Tighineanu et al., 2018). The visibility and dephasing rate can then be shown to be related by (González-Ruiz et al., 2022a)

$$V_{\text{HOM}} = \frac{\gamma}{\gamma + 2\gamma_d} , \tag{4.4}$$

where γ is the spontaneous decay rate of the quantum-dot. Additionally, slow drifts can make Alice and Bob's emitters go in and out of resonance over time. We neglect this effect for simplicity and assume that all photons are equally indistinguishable and that the limited visibility is only due to the fast dephasing rate γ_d.

Finally, we consider multi-photon emission, as characterised by the second order correlation function

$$g^{(2)} = \frac{2P_2}{(P_1 + 2P_2)^2} , \tag{4.5}$$

for a multiphoton state described by the density matrix

$$\hat{\rho} = \sum_k P_k \hat{\rho}_k , \tag{4.6}$$

where $\hat{\rho}_k$ represents the k-th photon component state with probability P_k and where $\sum_k P_k = 1$. We assume that $\hat{\rho} \simeq P_0\hat{\rho}_0 + P_1\hat{\rho}_1 + P_2\hat{\rho}_2 + \mathcal{O}(P_3)$, since for quantum-dot single-photon sources the probability of generating more than one photon is low. In fact we approximate all results to first order in P_2, such that we consider it to be very unlikely that two sources produce a two-photon state simultaneously ($P_2^2 \simeq 0$). Moreover the second-generated photon is assumed to be completely distinguishable from the other four. The presence of an extra photon in the set up thus induces an error that is effectively equivalent to having a detector dark count.

4.3 DIQKD protocol

We consider the scenario described in the previous section, where Alice and Bob are in secure laboratories and want to share a secret key. Furthermore, Alice and Bob only record their measurement when they receive a *yes* from the CHS. In our implementation, we consider a 2322 scenario where Alice has two measurement settings $x \in \{0,1\}$ and Bob has three settings $y \in \{0,1,2\}$, while both of them get two possible outcomes. In the following, we denote by x' and y' the key generating inputs, and we consider that an eavesdropper Eve has access to arbitrary quantum resources. The asymptotic rate r of a DIQKD protocol with one-way error correction is given by the Devetak-Winter bound (Devetak et al., 2005)

$$r \geq H(A|X=x',E) - H(A|B,X=x',Y=y')\,, \tag{4.7}$$

where $H(A|B)$ stands for the conditional von Neumann entropy of A given B.

From the statistics coming from the set-up described in the previous section, one can easily compute $H(A|B,X=x',Y=y')$. Thus, the main difficulty arises in bounding $H(A|X=x',E)$ knowing some statistical test $p(a_i,b_i|x_i,y_i) = c_i$ $\forall i \in \{0,1\}$. In Acín et al. (2007), an analytical lower bound on $H(A|X=x',E)$ was derived by considering a particular statistical test which is given by the CHSH inequality (Clauser et al., 1969). The robustness of the protocol with respect to losses has been improved using noisy prepossessing on Alice's side which can increase $H(A|X=x',E)$ more than $H(A|B,X=x',Y=y')$ (Ho et al., 2020). Recently, the authors of Brown et al. (2021) derived a convergent series of lower bounds on $H(A|X=x',E)$ where the statistical test is given by the value of the probabilities $p(a,b|x,y)$

$$H(A|X=x',E) \geq c_m + \sum_{i=1}^{m-1} \frac{w_i}{t_i \ln 2} \sum_a \inf_{Z_a \in B(E)} \Big\langle f(t_i, M_{a|x}, Z_{a,i}) \Big\rangle\,, \tag{4.8}$$

where the function $f(t_i, M_{a|x}, Z_{a,i})$ is defined as

$$f(t_i, M_{a|x}, Z_{a,i}) = M_{a|x}(Z_{a,i} + Z^*_{a,i} + (1-t_i)Z^*_{a,i}Z_{a,i}) + t_i Z^*_{a,i} Z^*_{a,i} \tag{4.9}$$

where w_i and t_i are the ith Gauss-Radau quadrature, such that increasing m leads to better bounds (see Brown et al. (2021) for details); and where $M_{a|x}$ and $N_{b|x}$ represent Alice's and Bob's POVM elements respectively, and $Z_{a,i}$ describes Eve's operators. In this expression, the following constraints need to be satisfied $\forall\ i \in \{0,1\}$, $\forall\ x \in \{0,1\}$, $\forall\ y \in \{0,2\}$:

$$\begin{aligned}
&\langle M_{a|x} N_{b|y} \rangle = p(a,b|x,y) \\
&\langle M_{a|x} \rangle = p(a|x), \quad \langle N_{b|y} \rangle = p(b|y), \\
&M_{a|x} > 0, \quad N_{b|y} > 0, M_{a|x}, N_{b|y} \text{ and } Z_{a,i} \in \mathrm{B(H)}.
\end{aligned} \tag{4.10}$$

The positivity of the POVM together with the condition $M_{a|x}$, $N_{b,y}$ and $Z_{a,i} \in$ B(H), where B(H) is the ensemble of bounded operators, can be relaxed using the Navascues-Pironio-Acín hierarchy (NPA) (Navascués et al., 2007; Navascués et al., 2008). In the following, we refer to such relaxation by OPT(m,A,B,x,y,t) with t the transmissivity of the beam splitter located in the CHS. Note that, usually, Alice uses her two settings both to test CHSH and generate the key, while Bob uses his two first settings to test CHSH and the third to generate the key. Here, we changed a bit the scenario and we allow Bob to use his three settings to compute an additional joint probability which will sometimes be used as an additional statistical test. We aim to find the best experimental parameters for DIQKD using single photon sources. To this end, we perform the numerical optimization

$$r = \max_{x,y}(\mathrm{OPT}(m, A, B, x, y) - H(A|B, X = x', Y = y')), \tag{4.11}$$

where the maximization runs over the possible experimental settings x and y, which in our case are determined by the measurement angles of Alice $(\theta_{A,0}, \theta_{A,1})$ and over the three measurement angles of Bob $(\theta_{B,0}, \theta_{B,1}, \theta_{B,2})$, and over the transmissivity t of the beam splitter at the CHS.

4.4 Results

In this section we present the results we obtained by solving the optimization problem presented in Eq. (4.3). We first compare it with other analytical techniques that have been developed in the literature (Ma et al., 2012; Ho et al., 2020; Brown et al., 2021), and then study the dependence of the key rate on the visibility V_{HOM} and the autocorrelation function $g^{(2)}$. Finally, we consider the scenario where Alice and Bob only have access to a limited number of rounds for generating the key. The details of the numerical implementation can be found in Appendix B.3.

4.4.1 Comparison with analytical formulas

Here, we compare the results of the optimization problem in Eq. (4.3) with the analytical bounds presented in Refs. (Ma et al., 2012; Ho et al., 2020). In both references, the bound is obtained by considering a similar 2322 scenario where Alice performs two measurements, Bob performs three measurements and they both get two outcomes. Two of Bob's measurements are used to optimize the CHSH inequality, while the outcomes of the third are used to construct the key between both parties. By doing this, Ma et al. (2012) found the following bound on the key rate

$$r \geq 1 - h\Big(\frac{1 + \sqrt{(S/2)^2 - 1}}{2}\Big) - H(B_2|A_0), \tag{4.12}$$

where $h(\cdot)$ represents the binary entropy and S corresponds to the CHSH score

$$S = E(x_0, y_0) + E(x_1, y_0) + E(x_0, y_1) - E(x_1, y_1)\,, \tag{4.13}$$

and where

$$E(x_d, y_q) = \sum_{i,j}(-1)^{i\oplus j} p(a_i, b_j|x_d, y_q)\,. \tag{4.14}$$

On the other hand, in Ho et al. (2020) the authors considered a different approach under which the data undergoes a preprocessing operation before being turned into

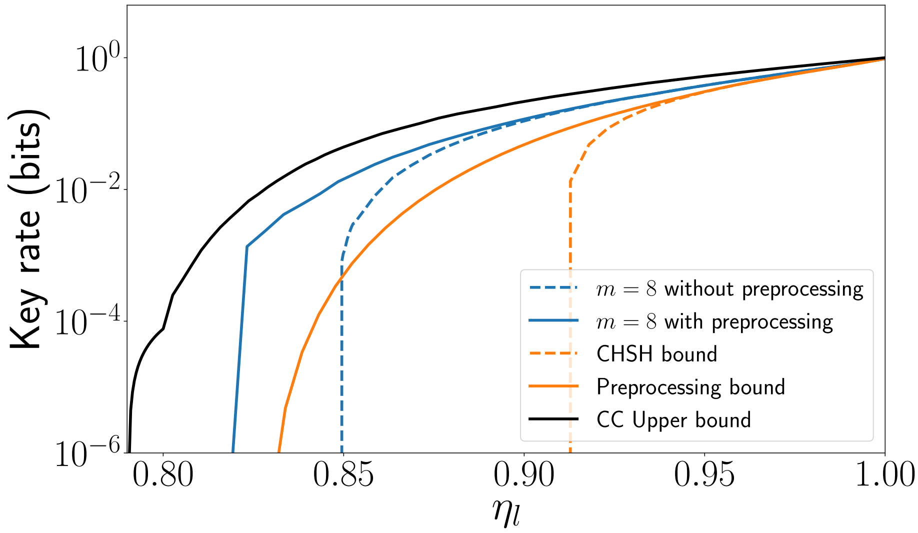


Figure 4.3: Dependence of the key rate on the detection efficiency η_l for the case of $V_{\mathrm{HOM}} = 1.0$ and $g^{(2)} = 0$. Here, we have set the transmission efficiency to $T = 10^{-3}$. In blue, we show the key rate obtained by solving the optimization problem in Eq. (4.3), where the solid (dashed) curve shows the rate obtained by (not) implementing the preprocessing strategy. In orange, we show the results obtained by using the analytical formulas in Eqs. (4.4.1) (dashed curve) and (4.15) (solid curve). The use of the optimization technique in general leads to better bounds on the obtained key rate, compared to the corresponding analytic bounds. These results coincide with those obtained in Brown et al. (2021). Finally, with the black solid curve we show an upper bound on the Devetak-Winter bound obtained by implementing the so-called Convex-Combination (CC) attack (Farkas et al., 2021; Łukanowski et al., 2022) using one-way communication reconciliation techniques.

the key. In particular, Alice performs a bit-flip operation on her outputs with probability q, which is equivalent to a change of her measurement operators from the set $\{M_0, M_1\}$ to $\{(1-q)M_0 + qM_1, qM_0 + (1-q)M_1\}$. Therefore, the bound of the key rate is given by

$$r \geq 1 - h\Big(\frac{1+\sqrt{(S/2)^2-1}}{2}\Big) - H(B_2|A_0) + h\Big(\frac{1+\sqrt{1-q(q-1)(8-S^2)}}{2}\Big), \quad (4.15)$$

where one can see that, depending on the CHSH score S, the introduction of the bit-flip operation q may increase Eve's ignorance on Alice's output more than Bob's. This strategy thus allows enhancing the rate obtained in Eq. (4.4.1). The same preprocessing technique can also be applied to our optimization problem in Eq. (4.3). The implementation of it, however, increases the number of variables we have to consider in the optimization.

With the aim of comparing the different techniques, we show in Fig. 4.3 the results for the ideal scenario $V_{\mathrm{HOM}} = 1.0$ and $g^{(2)} = 0.0$, i.e., where the photons generated by the quantum dots are completely indistinguishable and the generated state is pure. For now we consider the secret key rate per successful heralding event at the CHS. Hereupon, and unless otherwise stated, we therefore set the transmission efficiency to $T = 10^{-3}$ to investigate the limit where it has a negligible influence on the local efficiency. This will allow us to identify the minimal experimental requirements for obtaining a secret key (González-Ruiz et al., 2022a). We will later relax this assumption and investigate the influence of a higher transmission. The orange curves correspond to the bounds obtained from Eq. (4.4.1) (orange dashed curve) and Eq. (4.15) (orange solid curve), while blue curves show the solution found for the optimization problem presented in Eq. (4.3) when setting $m = 8$, with and without noisy preprocessing (blue solid and dashed curves, respectively). We see that, in both cases, the improved bound for the relative entropy between Alice and Eve shown in Eq. (4.8) allows for enhancing the final value of the key rate and lowers the limits for when this quantity starts to be positive. In particular, for the situation without noisy preprocessing we find that the key rate starts to be positive for $\eta_l > 0.909$, according to the analytic bound in Eq. (4.4.1), while the solution to Eq. (4.3) leads to $\eta_l > 0.848$. As η_l increases, the difference between both results becomes smaller, and they converge at $\eta_l = 1$ where $r \approx 1$ bit. On the other hand, the implementation of the noisy preprocessing strategy leads to an improvement with respect to the bound in Eq. (4.4.1), and provides positive values of the key rate for $\eta_l > 0.832$. Introducing this strategy at the level of Eq. (4.3) further reduces this limit to $\eta_l > 0.818$. Nevertheless, while the use of the noisy preprocessing truly improves the obtained bound on the efficiency, the differences in the key rate we get for $V_{\mathrm{HOM}} = 1.0$ are almost negligible in comparison with the ones obtained without implementing it. For instance, at $\eta_l = 0.848$, when the rate for the latter is already zero, the rate obtained with the noisy preprocessing is $r \approx 10^{-3}$ bits. We expect this improvement to be negligible in real experimental implementations, where finite statistics have to be considered. In the following and unless otherwise stated, we use Eq. (4.3) with $m = 8$ for the evaluation of the relative entropy between Alice and Eve. Finally, with the black curve we show an upper bound to the Devetak-Winter bound obtained by implementing the so-called Convex-Combination attack (Farkas et al., 2021; Łukanowski et al., 2022). As seen in the figure our results are close to the upper bound. This upper bound imposes a limit on what is the minimal value of η_l (in this case $\eta = 0.791$) for which one could potentially find positive key rates using one-way communication reconciliation techniques.

4.4.2 Dependence of the key rate on the distinguishability of the generated photons

As mentioned before, the HOM-visibility V_{HOM} determines how distinguishable the photons are. In typical experimental implementations with quantum-dot single-photon sources, the values of the visibility that can be achieved are around 96% (Tomm et al., 2021; Uppu et al., 2020). This parameter affects the quality of the generated states, leading to a reduction of the CHSH inequality violation for a fixed value of the local efficiency (González-Ruiz et al., 2022a). Thus, we expect its role to be fundamental for DIQKD implementations.

In Fig. 4.4, we show the dependence of the key rate on the local efficiency for three

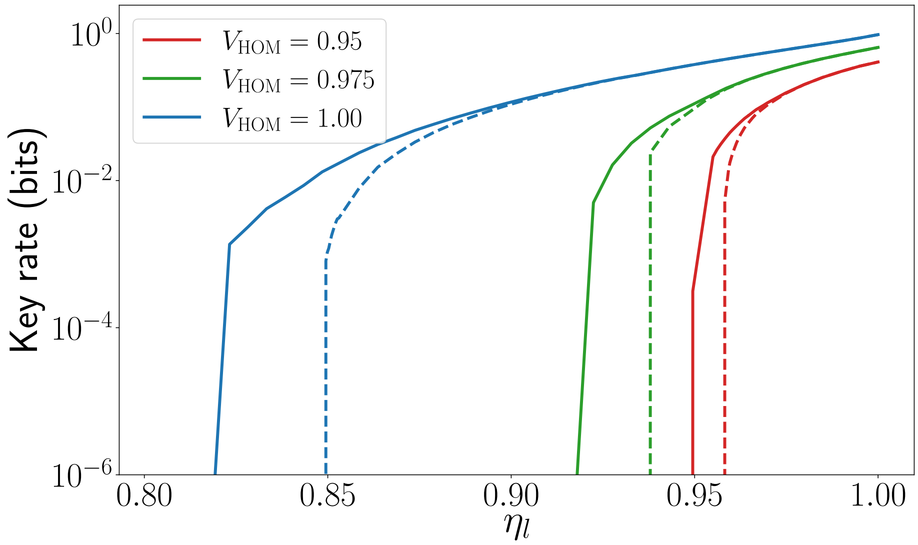


Figure 4.4: Dependence of the key rate on the visibility $V_{\rm HOM}$. Here, we have set $g^{(2)} = 0.0$ and the transmission efficiency to $T = 10^{-3}$. The solid curves show the key rate achieved when a noisy preprocessing strategy has been used for the generation of the key, while the dashed curves consider the case where the preprocessing has not been applied. In all curves, we have solved the optimization problem in Eq. (4.3) setting $m = 8$ and going up to second level in the NPA hierarchy (see Appendix B.3 for more details).

different values of the visibility, namely $V_{\rm HOM} = 0.95$ (red curves), $V_{\rm HOM} = 0.975$ (green curves) and $V_{\rm HOM} = 1.00$ (blue curves). In all cases we set $g^{(2)} = 0.00$. For a given value of the visibility, we show two curves: the dashed curve without the noisy preprocessing strategy, and the solid curve for which this strategy has been applied. As we observe, the introduction of the preprocessing strategy in general allows enhancing the key rate for small values of the local efficiency η_l, lowering the value of η_l for which they key starts to be positive. In particular, for $V_{\rm HOM} = 0.975$ we find that the key rate starts to be positive for $\eta_l > 0.918$ and $\eta_l > 0.938$ with and without the noisy preprocessing step respectively, while for $V_{\rm HOM} = 0.95$ we get $\eta_l > 0.949$ and $\eta_l > 0.958$. On the other hand, as $\eta \to 1$, the solid and dashed curves converge to the same value, and lead to $r = 0.648$ for $V_{\rm HOM} = 0.975$, and $r = 0.409$ for $V_{\rm HOM} = 0.95$.

4.4.3 Dependence of the key rate on the purity of the generated state

The probability of generating a second photon from the source can be quantified in terms of the second order autocorrelation function, as shown in Eq. (4.5). In experimental implementations, the degree of purity that can be attained is typically very high $g^{(2)} \leq 0.05$ (Tomm et al., 2021; Uppu et al., 2020). Nevertheless, and as it happens with the visibility, this quantity is also fundamental for establishing nonlocal correlations between Alice and Bob (González-Ruiz et al., 2022a), and therefore for generating a secure key between both parties.

In Fig. 4.5, we show the dependence of the key rate on the local efficiency for three

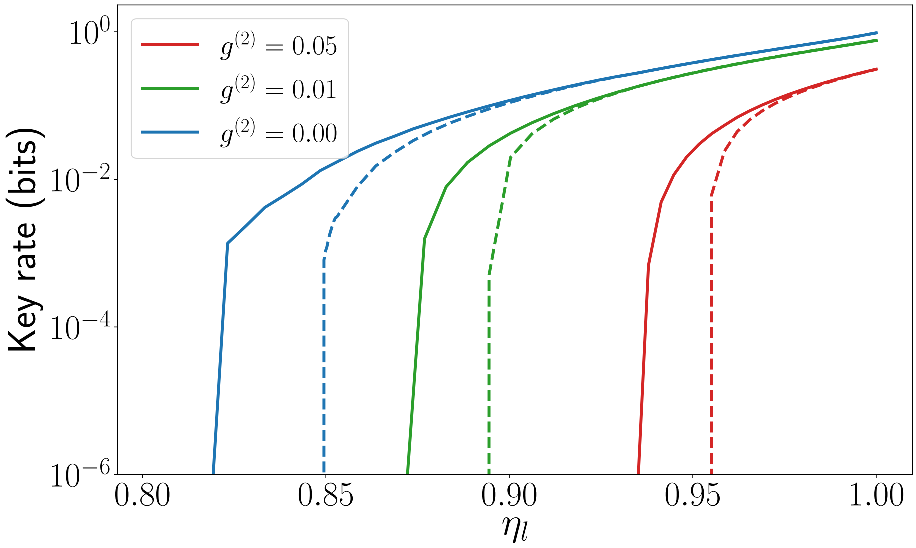


Figure 4.5: Dependence of the key rate on the autocorrelation function $g^{(2)}$ in log scale. Here, we have set $V_{\mathrm{HOM}} = 1.0$ and the transmission efficiency to $T = 10^{-3}$. The solid curves show the key rate achieved when a noisy preprocessing strategy has been used for the generation of the key, while the dashed curves consider the case where the preprocessing has not been applied. In all these curves, we have solved the optimization problem in Eq. (4.3) setting $m = 8$ and going up to second level in the NPA hierarchy (see Appendix B.3 for more information).

different values of the autocorrelation function, $g^{(2)} = 0.05$ (red curves), $g^{(2)} = 0.01$ (green curves) and $g^{(2)} = 0.00$ (blue curves). Here, we have set $V_{\mathrm{HOM}} = 1.00$. Similar to the visibility analysis, we show the situation where the noisy preprocessing strategy is (not) applied with solid (dashed) curves. We observed that, as it happens with the HOM-visibility, small modifications in the $g^{(2)}$ autocorrelation function have important consequences on the requirements for the detection efficiencies needed for obtaining positive values of the key rate. The noisy preprocessing strategy is, however, again useful for relaxing these requirements. In particular, we observe that for $g^{(2)} = 0.01$ we get positive key rates for $\eta_l > 0.872$ and $\eta_l > 0.894$ with and without the noisy preprocessing, respectively. On the other hand, for $g^{(2)} = 0.05$ the key rates starts to be positive for $\eta_l > 0.935$ and $\eta_l > 0.955$. Furthermore, in the limit of large efficiency ($\eta_l \to 1$), the solid and dashed lines converge to the same value, which is $r = 0.766$ for $g^{(2)} = 0.01$ and $r = 0.311$ for $g^{(2)} = 0.05$.

From the analysis we have done in this section, we observe that in the asymptotic limit of infinite rounds of the protocol, the main limiting factor in current experimental implementations lies in the local detection efficiency η_l. The limiting value of η_l for which the key rate becomes positive can be improved by means of noisy preprocessing techniques. For large values of η_l the difference with the *standard* protocol is, however, negligible. In the range of values for the visibility and second order autocorrelation function that is currently accessible experimentally for quantum dot single-photon sources ($V_{\mathrm{HOM}} \sim 0.96$, $g^{(2)} \leq 0.05$ (Tomm et al., 2021;

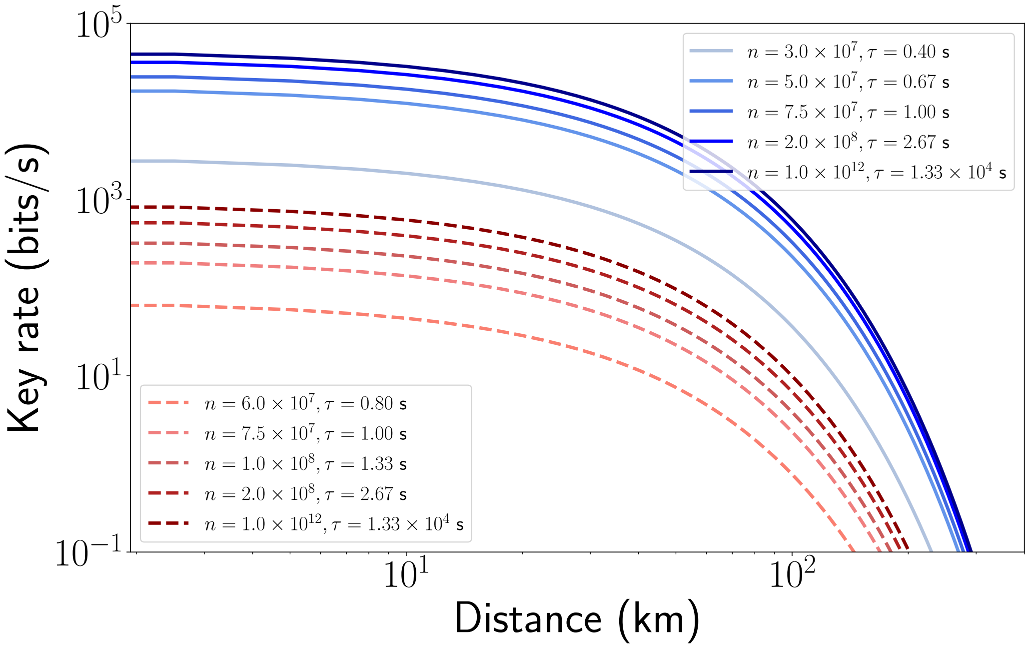


Figure 4.6: Key rate in bits per second as a function of the distance. We consider a single-photon source that generates photons at a rate of $\nu = 75$ MHz. The blue solid curves show the ideal case where $\eta_l = 1.0$, $V_{\mathrm{HOM}} = 1.0$ and $g^{(2)} = 0.00$. The red dashed curves show a more realistic case where $\eta_l = 0.957$, $V_{\mathrm{HOM}} = 0.975$ and $g^{(2)} = 0.01$. Each of the curves shown in the plot are obtained for different number of rounds n (see legend), such that the time required to perform this number of rounds is obtained as $\tau = n/\nu$. Here we have optimized the transmissivity of the beam splitter T for each set of experimental parameters. The optimal values are $T = 0.0622$ for the blue solid curves, and $T = 0.0106$ for the red dashed curves.

Uppu et al., 2020)), the key established between Alice and Bob starts to be secure for $\eta_l \gtrsim 0.9$. In the following, we consider a more realistic scenario where Alice and Bob have access to a limited amount of rounds n for the protocol, which adds an extra constraint to realistic DIQKD implementations.

4.4.4 Finite size analysis

Here, Alice and Bob only have access to a finite number of rounds n, which reduces the length l of secure key they can generate. On top of that, both parties are far away one from the other, and thus the photons that are sent to the CHS may be absorbed by the medium. In this section, we take these two experimental limitations into account. This allows us to provide a bound on the time and distance for which a secret key can be shared between Alice and Bob in photonic DIQKD experiments with quantum dots.

A recent breakthrough regarding the computation of key rates for finite statistics is the entropy accumulation theorem (EAT) (Dupuis et al., 2020). The EAT bounds the amount of randomness generated by two parties ($\mathrm{Rand}_{\text{Alice-Bob}}$) in n rounds against an arbitrary powerful quantum adversary Eve given a statistical test, here the CHSH score S, according to

$$\text{Rand}_{\text{Alice-Bob}} \geq nh(S) - \sqrt{n}k \tag{4.16}$$

where $h(S)$ is the worst-case von Neumann entropy of an individual round of the protocol with expected score S, and k is a correction factor which comes from the finite statistics. The length of the key is then given by the difference between the amount of entropy certified by the EAT, and the amount of information shared in the classical message during privacy amplification and error correction. We follow the approach of Tan et al. (2020), for bounding the single round von Neumann entropy (Liu et al., 2021; Nadlinger et al., 2022). Therefore, Theorem 1 in Tan et al. (2020) allows us to obtain an upper bound on the length l of the secure key that we are able to generate with the presented protocol. The length l is linked to the key rate by the number of protocol rounds n that Alice and Bob undergo, i.e. $r = l/n$, such that in the asymptotic limit $n \to \infty$ we recover Eq. (4.4.1).

In realistic experimental implementations, the number of rounds is usually determined by the rate at which the single-photon source generates photons, and the amount of time Alice and Bob spend running the protocol to generate the key. In typical quantum dot implementations, the rate is typically around $\nu = 75$ MHz (Uppu et al., 2020; Tomm et al., 2021; Wang et al., 2019). Furthermore, in order to consider one out of the n protocol rounds to be successful, Alice and Bob need to get a positive response from the CHS. Therefore, the distance between both parties is a key aspect to take into account. Large distances between Alice and Bob lead to a decreasing probability of heralding, as it is more likely for the heralding photon to get lost on its route to the CHS. In general, the transmission efficiency can be written as

$$\eta_t = e^{-\frac{L}{2L_0}}, \tag{4.17}$$

where L is the distance between Alice and Bob and L_0 is the attenuation length of the media through which the light travels (the factor of two arises because the distance to the CHS is only half the distance between Alice and Bob). For optical fibers at the telecommunication wavelength a typical value is $L_0 = 22$ km. Thus, the transmission efficiency η_t affects the probability of heralding P_h, which we get by summing all the probability terms that correspond to acceptance from the CHS (see Table 4.1). These terms already account for all possibilities of emission of a second-generated photon when $g^{(2)} \neq 0$. We note that this probability is as well a function of the beam splitter transmittance T (see Fig. 4.1), such that small values of T lead to low values of the heralding probability but to higher asymptotic key rates per successful heralding, as we reduce the chance of sending two photons to the CHS. On the other hand, big values of T increase the heralding probability at the cost of reducing the security of the key. Thus, in order to establish long enough keys between Alice and Bob, the probability of heralding, and therefore the transmissivity T, plays a fundamental role.

In Fig. 4.6, we show the dependence of the key rate (in bits per second) as a function of the distance for different experimental parameter when using a quantum dot single-photon source that generates photons with a rate of $\nu = 75$ MHz. We have followed Tan et al. (2020) in order to perform the finite size analysis, and we have imposed our protocol to be 10^{-2}-sound and 10^{-6}-complete (see Tan et al. (2020) for definition). In particular, with the blue solid curves we consider an ideal scenario where $\eta_l = 1.0$, $V_{\text{HOM}} = 1.00$ and $g^{(2)} = 0.00$. On the other hand, the red dashed curves present a more realistic scenario where $\eta_l = 0.957$, $V_{\text{HOM}} = 0.975$ and $g^{(2)} = 0.01$. Each of the curves shown in the figure correspond to a different number of protocol rounds n used by Alice and Bob for generating the key (see legends). Here, $\tau = n/\nu$ corresponds to the time it takes a single-photon source that generates photons with rate $\nu = 75$ MHz to perform n rounds of the protocol. For both kind of curves (blue solid and red dashed), we observe that the bigger n is, the higher the key rate. Furthermore, in both cases we find that for $n \leq 10^7$ it is not possible to extract a key, according to the soundness and completeness requirements that we use. An increase in the number of rounds leads to larger values of key rate, up to a maximum value that corresponds to the asymptotic regime which we represent with the cases where $n = 10^{12}$ (shown with the darkest solid and dashed curves). Running this number of rounds takes on the order of $\tau \sim 10^4$ seconds when using a source that generates photons with a rate of $\nu = 75$ MHz. However, we observe that with $\tau \sim 1$ s, Alice and Bob could obtain key rates comparable to those found in the asymptotic regime.

Unlike the plots shown in the previous section, in Fig. 4.6 we have considered an extra optimization over the transmissivity T of the beam splitter in each of Alice's and Bob's stations, assuming them to be equal. This way, we can increase the probability of heralding P_h up to the order of 10^{-2}, allowing us to obtain secure keys at longer distances after a limited time. In particular, we observe that in the worst of the considered scenarios, i.e. the red dashed curves, the key rate reduces to 0.1 bits/s at a range of distances $L \in [144, 200]$ km (the limits obtained for $n = 6.0 \times 10^7$ and $n = 10^{12}$ rounds respectively). On the other hand, for the ideal case we find the same key rate for distances $L \in [230, 292]$ km (the limits obtained for $n = 3.0 \times 10^7$ and $n = 10^{12}$ rounds respectively). Therefore, the increase of the heralding probability allows establishing secure rates for longer distances, at the cost of reducing the length of key per second. An alternative approach would be to increase the repetition rate ν of the single-photon source, although it might require more effort from the experimental side.

4.5 Conclusion

We have used new theoretical tools to evaluate the experimental requirements in order to perform DIQKD using single-photon sources in a heralded scheme. We focused on the parameters which are routinely used to characterize single-photon sources, such as the time-zero second order correlation function $g^{(2)}$, the HOM visibility V_{HOM} and the local detection efficiency η_l of the source. We have computed the asymptotic key rate using the novel method of Brown et al. (2021) for bounding the relative entropy between Alice and Eve, and we showed that this improves the analytical bounds obtained in Refs. (Ma et al., 2012; Ho et al., 2020). Finally, we considered a situation where the number of rounds for obtaining a secure key rate is limited, i.e., a finite statistics analysis. We studied the time and distance requirements needed to establish a secure rate between Alice and Bob with realistic parameters obtainable with quantum dot single-photon sources. However, although we have focused on single-photon sources using quantum dots, the methods we have employed can be trivially extended to any other single-photon source.

Our analysis improves the experimental requirements for performing DIQKD with single-photon sources, and we reach numbers which are within reach for near-future experimental implementations. We believe that our work represents a strong motivation for the improvement of existing single-photon sources, so that they can be used to perform DIQKD. A step towards this implementation could be to relax the assumptions that Alice and Bob do not have knowledge on their device, or to allow Eve for less general attacks. This would lead to more relaxed experimental requirements.

Chapter 5

The single-photon stretcher

This chapter is based on preliminary and unpublished results from a project currently in progress. The objective is to be able to store the quantum information encoded in single-photons into high-Q optomechanical membranes. These quantum oscillators have reported to have up to ms coherence times (Rossi et al., 2018; Seis et al., 2022). The challenge resides in that while the usual single-photon pulse length ranges in the pico-second scale (Uppu et al., 2020), optomechanical quantum memories oscillate in the range of MHz. This creates a bandwidth mismatch of between four and six orders of magnitude between the timescale of the two systems. In simpler words, by the time the membrane starts to sense the interaction with

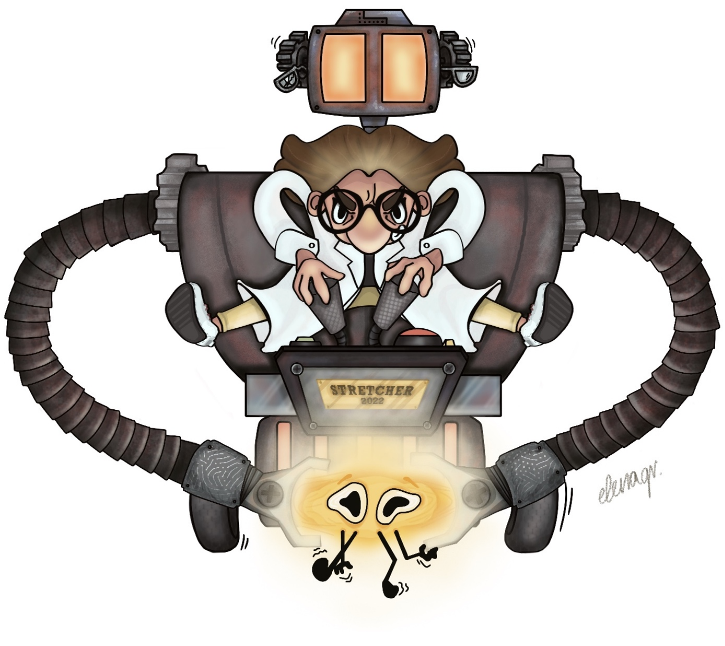


Figure 5.1: Artist's impression of the single-photon stretcher. Credits: Elena González Ruiz (2022).

the single-photon, the pulse carrying the qubit is already gone. As a solution, we propose to use a cavity and a non-linear crystal as an effective stretcher of the photon pulse length to coherently extend the interaction time between the memory and the photonic qubit. That is, the photon stretcher will effectively narrow the original bandwidth of the photon such that it can fit the bandwidth of the mechanical membrane, ideally at a low efficiency cost.

5.1 Introduction

The basic idea behind the single-photon stretcher is to place a high-efficiency non-linearity (NL) inside of a optical cavity at a specific position. This non-linear material can be for instance a non-linear crystal (Da Lio et al., 2022), and it must have relatively low losses for the conversion to succeed. The functioning principle of the stretcher then consists on that the NL will adiabatically decrease the frequency of the single-photon with each iteration in the cavity, until it has been completely ”stretched" (see Fig. 5.1 for an artistic impression). However, no NL has perfect efficiency (and neither does the cavity), and thus the longer the photon stays inside of the cavity the more likely it will be that it will be lost before successfully exiting the stretcher. Therefore the main goal of the study is to find the optimal cavity parameters such that the photon stays in the cavity an optimal amount of time, given the relevant realistic imperfections of the system.

To estimate the capabilities of such an implementation before proceeding with the detailed analysis, let us make a short calculation. The ratio χ between the the single-photon pulse length T and the characteristic response time of the membrane τ is the quantity that we wish to enhance with the set up, which in terms of the membrane narrow bandwidth $\Delta\omega = 1/\tau$ is just

$$\chi = \Delta\omega T\,. \tag{5.1}$$

On the other hand, we calculate the same ratio after the effect of the stretcher (χ'). The stretched pulse length will be inversely proportional to the cavity coupling rate κ, thus

$$\chi' = \frac{\Delta\omega}{\kappa/(2\pi)}\,, \tag{5.2}$$

The total coupling has the contributions $\kappa = \kappa_{\text{loss}} + \kappa_{\text{out}}$, this is, the rates at which photons are lost and correctly out-coupled, respectively. If we look at the probability P_{out} to couple out of the cavity

$$P_{\text{out}} = \frac{\kappa_{\text{out}}}{\kappa_{\text{loss}} + \kappa_{\text{out}}}\,, \tag{5.3}$$

we see that the maximum out-coupling probability is ensured when $\kappa_{\text{loss}} = \kappa_{\text{out}}$[1]. Furthermore, when the round-trip time inside of the cavity $1/\nu_{\text{FSR}}$ (ν_{FSR} being

[1] This is commonly known as a limit in which the cavity is *critically coupled.*

the cavity's free spectral range) equals the input pulse length, i.e. $1/\nu_{\mathrm{FSR}} = T$, the neighbouring longitudinal modes, one free spectral range away of the resonant frequency, of the cavity begin to get populated (see Fig. [X]). This bad case scenario is thus the limit for our optimal conversion for a certain cavity size L. We finally define the stretching factor η and substitute these values, obtaining

$$\eta \equiv \frac{\chi'}{\chi} \leq \frac{2\pi\Delta\omega/\kappa}{\Delta\omega(1/\nu_{\mathrm{FSR}})} = \frac{2\pi\nu_{\mathrm{FSR}}}{\kappa} = \mathcal{F}\,, \tag{5.4}$$

where $\mathcal{F}$ is the finesse of the cavity. This is great news: we can expect a bandwidth conversion of several orders of magnitude, upper bounded by the finesse of the cavity. In the following sections we perform the detailed calculations where we present the subtleties of this quick, hand-wavy initial result. In particular, we will show how the adiabatic conditions are in fact hard to fulfill, which is simplified by assuming a certain amount of losses in order to be able to perform perturbation theory, and how the coupling to neighboring longitudinal modes limits the stretching parmeter.

5.2 Analysis

We start by defining the cavity mode as $\hat{a}(t)$, while the photons from the input pulse (those to be stretched) are defined to be in the mode $\hat{b}(t)$. For simplicity we model the input photons to be in a second cavity perpendicular to the actual optical cavity from the set-up (see Fig. 5.2). This picture is valid since we assume the $\hat{b}(t)$ mode to be off-resonant with respect to the optical cavity. From the input-output formalism (Walls et al., 2008, p. 131) we know that the time evolution of the two modes $\hat{a}(t)$ and $\hat{b}(t)$ satisfies

$$\begin{aligned} \dot{\hat{a}}(t) &= \frac{-i}{\hbar}[\hat{a}(t),\hat{H}] - \frac{\kappa_a}{2}\hat{a}(t) + \sqrt{\kappa_{\mathrm{out},a}}\hat{a}_{in}(t), \quad \hat{a}_{in}(t) + \hat{a}_{\mathrm{out}}(t) = \sqrt{\kappa_{\mathrm{out},a}}\hat{a}(t) \\ \dot{\hat{b}}(t) &= \frac{-i}{\hbar}[\hat{b}(t),H] - \frac{\kappa_b}{2}\hat{b}(t) + \sqrt{\kappa_{\mathrm{out},b}}\hat{b}_{in}(t), \quad \hat{b}_{in}(t) + \hat{b}_{\mathrm{out}}(t) = \sqrt{\kappa_{\mathrm{out},b}}\hat{b}(t)\,, \end{aligned} \tag{5.5}$$

where $\hat{H}$ is the system's Hamiltonian and the total decay rates κ_a and κ_b are given by

$$\kappa_a = \kappa_{\mathrm{out},a} + \kappa_{\mathrm{loss}}, \quad \kappa_b = \kappa_{\mathrm{out},b} + \kappa_{\mathrm{loss}}\,, \tag{5.6}$$

where $\kappa_{\mathrm{out},i}$ $(i = a, b)$ is the rate at which photons couple out from the cavity and κ_{loss} expresses the rate at which photons from either modes are lost. We further assume that there are no input photons in the cavity mode ($\hat{a}_{in}(t) = 0$) since the only input will be the photons to be bandwidth matched, and that no output photons will remain in the off-resonant mode ($\hat{b}_{\mathrm{out}}(t) = 0$), yielding the relations

$$\hat{a}_{\mathrm{out}}(t) = \sqrt{\kappa_{\mathrm{out},a}}\hat{a}(t), \quad \hat{b}_{in}(t) = \sqrt{\kappa_{\mathrm{out},b}}\hat{b}(t)\,. \tag{5.7}$$

The objective is thus to design an optimal cavity such that the total cavity output field $\hat{a}_{\mathrm{out}}(t)$ has the biggest number of photons with the desired bandwidth. On the

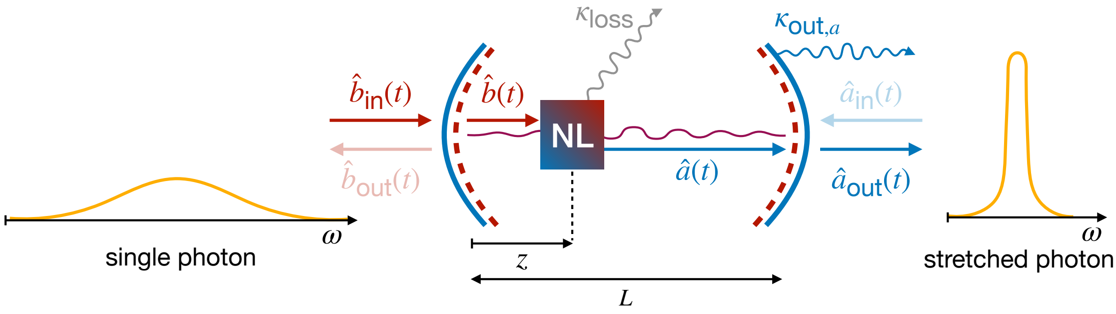


Figure 5.2: Scheme of the functioning of the photon stretcher set-up. The cavity mode $\hat{a}(t)$ is resonant with the optical cavity (all in blue), while the $\hat{b}(t)$ modes are only resonant with the fictitious cavity represented in dashed lines (in red). The cavity has a length L and the non-linearity (NL) is placed at a position z. The most relevant coupling rates are also shown in the picture.

other hand, the Hamiltonian of the system is given by

$$\hat{H} = \hbar \sum_i \omega_{a,i} \hat{a}_i^\dagger \hat{a}_i + \hbar \omega_b \hat{b}^\dagger \hat{b} + \hbar \sum_i \left(\Omega(t) \hat{a}_i^\dagger \hat{b} + \Omega(t)^* \hat{b}^\dagger \hat{a}_i \right) , \tag{5.8}$$

where we have included the field Hamiltonians of the cavity field ($\sum_i \omega_{a,i} \hat{a}_i^\dagger \hat{a}_i$) and the input field ($\hbar \omega_b \hat{b}^\dagger \hat{b}$), together with the interaction Hamiltonian where $\Omega(t)$ acts as the coupling constant through the NL between the two. The frequencies $\omega_{a,i}$ ($i = \pm\infty$) and ω_b are thus the resonant frequencies of each photonic mode. The interaction between the two fields occurs by means of the NL, therefore we can interpret $\Omega(t)$ as a pulse shape we can optimise over in order to maximise the efficiency of the process. Note that we have assumed the input field to be single-mode, while the cavity one is multimode. This will allow us to model the realistic imperfection of coupling the cavity field to undesired modes beyond the resonant one.

The total output field from the cavity $\hat{a}_{\text{out}}(t)$ has two different contributions, as explained above: the single mode $\hat{a}_{\text{out},SM}(t)$, that corresponds to the resonant mode of the cavity with frequency $\omega_{a,0}$ (this is, ideally, the only mode we would like to couple to), and the multimode component $\hat{a}_{\text{out},MM}(t)$, that represents the rest of the cavity modes. Therefore the total output cavity mode is given by

$$\hat{a}_{\text{out}}(t) = \hat{a}_{\text{out},SM}(t) + \hat{a}_{\text{out},MM}(t) \, . \tag{5.9}$$

These separation into single-mode and multimode contributions will be very useful for understanding the effect of imperfections in the following sections. We can now calculate the total number of stretched photons N

$$N \equiv \int_{\infty}^{\infty} d\omega \hat{a}_{\text{out}}^\dagger(\omega) \hat{a}_{\text{out}}(\omega) \simeq \int_{-\Delta\omega/2}^{\Delta\omega/2} d\omega \hat{a}_{\text{out}}^\dagger(\omega) \hat{a}_{\text{out}}(\omega) \, , \tag{5.10}$$

where $\Delta\omega$ is the bandwidth, that we have assumed to be narrow. The number of photons N is the quantity that we want to maximise, for which we will optimise the different cavity parameters. The expression above has different contributions

$$N = \int_{-\Delta\omega/2}^{\Delta\omega/2} d\omega \Big(\hat{a}^\dagger_{\text{out},SM}(\omega)\hat{a}_{\text{out},SM}(\omega) + \hat{a}^\dagger_{\text{out},MM}(\omega)\hat{a}_{\text{out},MM}(\omega) \\ + (\hat{a}^\dagger_{\text{out},MM}(\omega)\hat{a}_{\text{out},SM}(\omega) + \text{H.c.}) \Big) , \quad (5.11)$$

that we calculate separately in the following subsections.

5.2.1 Single-mode contribution

For the analysis of this contribution we can simplify the Hamiltonian from Eq. 5.8 to

$$\hat{H} = \hbar\omega_{a,0}\hat{a}^\dagger\hat{a} + \hbar\omega_{b,0}\hat{b}^\dagger\hat{b} + \hbar\left(\Omega(t)\hat{a}^\dagger\hat{b} + \Omega(t)^*\hat{b}^\dagger\hat{a}\right) . \quad (5.12)$$

We then switch to a rotating frame around the driving frequencies $\omega'_{a,0}$ and $\omega'_{b,0}$, detuned $\Delta_a = \omega_{a,0} - \omega'_{a,0}$ and $\Delta_b = \omega_{b,0} - \omega'_{b,0}$ from the resonant mode frequencies. That is, we change to the interaction picture Hamiltonian by applying the following transformation to Eq. (5.12)

$$\hat{H}' = e^{i\hat{H}_0 t/\hbar}\hat{H}e^{-i\hat{H}_0 t/\hbar} - \hat{H}_0 , \quad (5.13)$$

where we have defined $\hat{H}_0 = \hbar\omega'_{a,0}\hat{a}^\dagger\hat{a} + \hbar\omega'_{b,0}\hat{b}^\dagger\hat{b}$. Thus the Hamiltonian in the rotating field is

$$\hat{H}' = \hbar\Delta_a\hat{a}^\dagger\hat{a} + \hbar\Delta_b\hat{b}^\dagger\hat{b} + \hbar\left(\tilde{\Omega}(t)\hat{a}^\dagger\hat{b} + \tilde{\Omega}(t)^*\hat{b}^\dagger\hat{a}\right) , \quad (5.14)$$

where we have defined the rotating-frame coupling constant $\tilde{\Omega}(t)$ as

$$\tilde{\Omega}(t) = \Omega(t)e^{i\left(\omega_{a,0}-\Delta_a-(\omega_{b,0}-\Delta_b)\right)t} . \quad (5.15)$$

We can then insert the rotating-frame Hamiltonian from Eq. 5.14 in Eqs. 5.5, obtaining

$$\begin{aligned} \dot{\hat{a}}(t) &= -\left(i\Delta_a + \frac{\kappa_a}{2}\right)\hat{a}(t) - i\tilde{\Omega}(t)\hat{b}(t), \quad \hat{a}_{\text{out}}(t) = \sqrt{\kappa_{\text{out},a}}\hat{a}(t) \\ \dot{\hat{b}}(t) &= -\left(i\Delta_b + \frac{\kappa_b}{2}\right)\hat{b}(t) - i\tilde{\Omega}^*(t)\hat{a}(t) + \sqrt{\kappa_{\text{out},b}}\hat{b}_{in}(t), \quad \hat{b}_{in}(t) = \sqrt{\kappa_{\text{out},b}}\hat{b}(t) . \end{aligned} \quad (5.16)$$

Solving above's system of coupled differential equations in general is quite difficult. We simplify the system by adiabatically eliminating the cavity for the control mode $\hat{b}(t)$, since it is not resonant with the cavity and is therefore a very lossy mode in comparison with the resonant mode $\hat{a}(t)$ ($\kappa_b \gg \kappa_a$). In other words, we identify $\hat{a}(t)$ as variable that varies very slowly in time compared to $\hat{b}(t)$. We can thus use the result for adiabatic elimination of a fast variable $x_2(t)$ respect to a slow variable $x_1(t)$ related by

$$\begin{aligned}\dot{x}_1 &= \kappa_1 f_1(x_1, x_2),\\ \dot{x}_2 &= \kappa_2 f_2(x_1, x_2),\end{aligned} \tag{5.17}$$

that in the limit where $\kappa_2 \gg \kappa_1$ has the solution

$$x_2(t) = g_2(x_1(t), x_2(t)) \int_0^{t-t_0} e^{-\kappa_2 \tau} d\tau = \frac{1}{\kappa_2} g_2(x_1(t), x_2(t)) , \tag{5.18}$$

where $g_2(x_1, x_2) = \kappa_2 f_2(x_1, x_2) + \kappa_2 x_2$ (Lugiato et al., 2015, p. 106). We apply above's result to adiabatically eliminate the control mode $\hat{b}(t)$, obtaining

$$\hat{b}(t) \simeq \frac{1}{i\Delta_b + \frac{\kappa_b}{2}} \left(\sqrt{\kappa_{\text{out},b}} \hat{b}_{in}(t) - i\tilde{\Omega}^*(t)\hat{a}(t) \right) . \tag{5.19}$$

Now we plug this approximation into Eqs. 5.35 and solve the differential equation similarly to that solved in [Meystre & Sargent] to get

$$\begin{aligned}\hat{a}_{\text{out}}(t) = -i\frac{\sqrt{\kappa_{\text{out},a}\kappa_{\text{out},b}}}{i\Delta_b + \frac{\kappa_b}{2}} \int_{t_0}^{t} dt' \hat{b}_{in}(t')\tilde{\Omega}(t') \cdot \\ \exp\left\{ -\left(i\Delta_a + \frac{\kappa_a}{2} \right)(t - t') - \frac{1}{i\Delta_b + \frac{\kappa_b}{2}} \int_{t'}^{t} d\tau |\Omega(\tau)|^2 \right\},\end{aligned} \tag{5.20}$$

where we have assumed that there was no field present in the cavity prior to the initial time t_0, i.e., $\hat{a}(t_0) = 0$. Since the mode $\hat{a}(t)$ varies very slowly compared to $\hat{b}(t)$, the input pulse $\hat{b}(t)$ is much shorter than the cavity decay time, and therefore we can approximate that the term $\exp\left\{ -\left(i\Delta_a + \frac{\kappa_a}{2} \right)(t - t') \right\}$ can be pulled out of the integral. We thus obtain that

$$\hat{a}_{\text{out}}(t) \simeq -i\frac{\sqrt{\kappa_{\text{out},a}\kappa_{\text{out},b}}}{i\Delta_b + \frac{\kappa_b}{2}} e^{-\kappa_a(t-t_0)/2} \int_{t_0}^{t} dt' \hat{b}_{in}(t')\tilde{\Omega}(t') \exp\left\{ -\frac{1}{i\Delta_b + \frac{\kappa_b}{2}} \int_{t'}^{t} d\tau |\Omega(\tau)|^2 \right\}, \tag{5.21}$$

where we have omitted a global phase from $i\Delta_a$ as it can be easily compensated by the phase choice of $\tilde{\Omega}(t)$.

In Eq. (5.21) we can see how a smart choice of the pulse shape $\Omega(t)$ directly influences the output field from the cavity $\hat{a}_{\text{out}}(t)$. Let us then solve how $\Omega(t)$ should ideally be to fully overlap with the mode $\hat{b}_{in}(t)$ in Eq. (5.21) and thus maximise the single-mode contribution to the N number of stretched output photons. For this calculation we partially follow the method presented in Gorshkov et al. (2007). We start by defining the wavefunction $\psi(t', t)$ as

$$\psi(t', t) \equiv \frac{\sqrt{\kappa_b}}{i\Delta_b + \frac{\kappa_b}{2}} \tilde{\Omega}(t') \exp\left\{ -\frac{1}{i\Delta_b + \frac{\kappa_b}{2}} \int_{t'}^{t} d\tau |\Omega(\tau)|^2 \right\} . \tag{5.22}$$

We then evaluate $|\psi(t',t)|^2$ at a finite time T, that corresponds to the total pulse length. We do so in order to avoid normalisation problems later on in the calculation. We obtain

$$|\psi(t',T)|^2 = \frac{\kappa_b}{\Delta_b^2 + (\frac{\kappa_b}{2})^2}|\Omega(t')|^2 \exp\left\{-\frac{\kappa_b}{\Delta_b^2 + (\frac{\kappa_b}{2})^2}\int_{t'}^{T} d\tau|\Omega(\tau)|^2\right\}. \tag{5.23}$$

We then integrate above's expression from the initial time t_0 until a time $t < T$, yielding

$$\begin{aligned}\int_{t_0}^{t} dt'|\psi(t',T)|^2 &= \int_{t_0}^{t} dt' \frac{\kappa_b}{\Delta_b^2 + (\frac{\kappa_b}{2})^2}|\Omega(t')|^2 \exp\left\{-\frac{\kappa_b}{\Delta_b^2 + (\frac{\kappa_b}{2})^2}\int_{t'}^{T} d\tau|\Omega(\tau)|^2\right\} \\ &= \exp\left\{-\frac{\kappa_b}{\Delta_b^2 + (\frac{\kappa_b}{2})^2}\int_{t}^{T} d\tau|\Omega(\tau)|^2\right\} \\ &\qquad - \exp\left\{-\frac{\kappa_b}{\Delta_b^2 + (\frac{\kappa_b}{2})^2}\int_{t_0}^{T} d\tau|\Omega(\tau)|^2\right\}, \end{aligned} \tag{5.24}$$

where we have applied the fundamental theorem of calculus[2] to solve the integration of the exponential term. Since the pulses are normalised such that they diverge when integrated over the whole pulse length $\int_{t_0}^{T} d\tau|\Omega(\tau)|^2 \to \infty$, the second term of the integral equals 0 and thus we get that

$$\int_{t_0}^{t} dt'|\psi(t',T)|^2 = \exp\left\{-\frac{\kappa_b}{\Delta_b^2 + (\frac{\kappa_b}{2})^2}\int_{t}^{T} d\tau|\Omega(\tau)|^2\right\}, \tag{5.25}$$

which indeed shows a correct normalisation when $t = T$, as $\int_{t_0}^{t} dt'|\psi(t',T)|^2 = 1$. The last step in the calculation is to isolate the integral of the modulus squared of the pulse $\tilde{\Omega}(t)$ and derive the expression with respect to the time t to finally obtain

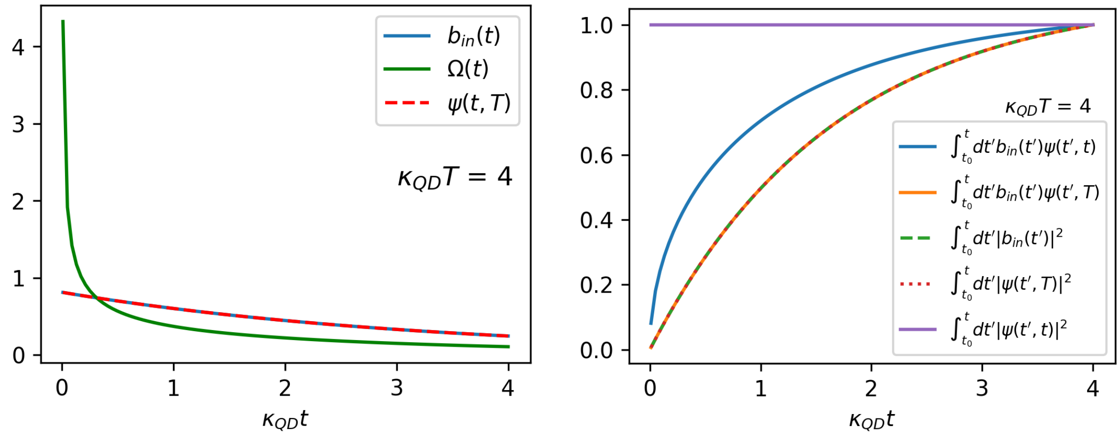
$$|\Omega(t)| = \sqrt{\frac{\Delta_b^2 + (\frac{\kappa_b}{2})^2}{\kappa_b}}\frac{|\psi(t,T)|}{\sqrt{\int_{t_0}^{t} dt'|\psi(t',T)|^2}}. \tag{5.26}$$

We can see that this expression intuitively makes sense, as it diverges when time is evaluated at the initial time $t = t_0$ as expected. Note that we are still missing the calculation of the phase of the coupling pulse, since Eq. (5.26) only allows for calculating the modulus $|\Omega(t)|$. However, since the wavefunction $\psi(t',t)$ is known, it can easily be obtained from Eq. (5.22).

The overlap between $\hat{b}_{in}(t)$ and $\psi(t',t)$ can therefore be perfect when choosing the appropriate pulse shape $\Omega(t)$ according to the solution found in Eq. (5.26), as we can see in Fig.5.3. In other words, we can choose $\psi(t',T)$ such that

$$\int_{t_0}^{T} dt'\hat{b}_{in}(t')\psi(t',T) = 1 \quad \Rightarrow \quad \hat{a}_{\text{out},SM}(t) = -i\sqrt{\frac{\kappa_{\text{out},a}\kappa_{\text{out},b}}{\kappa_b}}e^{-\kappa_a(t-t_0)/2}, \tag{5.27}$$

[2] i.e. $\frac{d}{dx}\left(\int_a^x f(t)dt\right) = f(x)$.



(a) (b)

Figure 5.3: (a) Plot of the different wavefunctions involved in the optimisation of the number of single-mode cavity photons for $t_0 = 0$ and $T = 4$. The input pulse $\hat{b}_{in}(t)$ is perfectly reproduced by $\psi(t,T)$ for the choice of driving $|\Omega(t)|$ derived in equation 5.26. (b) In this plot we check the normalisation of the different wavefunctions plotted in (a), as well as their crossed terms, for $t_0 = 0$ and $T = 4$.

which maximises the output field from Eq. (5.21).

Finally we would like to calculate the optimal number of stretched photons when we choose the optimal pulse $|\Omega(t)|$. We take the Fourier transform of the output cavity mode obtained in Eq. 5.27, yielding

$$\hat{a}_{\text{out},SM}(\omega) = -i\sqrt{\frac{\kappa_{\text{out},a}\kappa_{\text{out},b}}{2\pi\kappa_b}}\int_{t_0}^{\infty} dt e^{-\kappa_a(t-t_0)/2+i\omega t} = -i\sqrt{\frac{\kappa_{\text{out},a}\kappa_{\text{out},b}}{2\pi\kappa_b}}\frac{1}{\frac{\kappa_a}{2}-i\omega}e^{i\omega t_0}\,. \tag{5.28}$$

Therefore the single-mode contribution to the total number of photons N (Eq. (5.11)) is

$$\begin{aligned}\int_{-\Delta\omega/2}^{\Delta\omega/2} d\omega \hat{a}^{\dagger}_{\text{out},SM}(\omega)\hat{a}_{\text{out},SM}(\omega) &= \frac{\kappa_{\text{out},a}\kappa_{\text{out},b}}{2\pi\kappa_b}\int_{-\Delta\omega/2}^{\Delta\omega/2}\frac{1}{(\frac{\kappa_a}{2})^2+\omega^2}d\omega \\ &= \frac{\kappa_{\text{out},a}\kappa_{\text{out},b}}{2\pi\kappa_b}\left[\frac{2\arctan 2\omega/\kappa_a}{\kappa_a}\right]_{-\Delta\omega/2}^{\Delta\omega/2},\end{aligned} \tag{5.29}$$

which for a small bandwidth $\Delta\omega$ can be approximated by

$$\int_{-\Delta\omega/2}^{\Delta\omega/2} d\omega \hat{a}^{\dagger}_{\text{out},SM}(\omega)\hat{a}_{\text{out},SM}(\omega) \simeq \frac{\kappa_{\text{out},a}\kappa_{\text{out},b}}{2\pi\kappa_b}\left[\frac{4\omega}{\kappa_a^2}\right]_{-\Delta\omega/2}^{\Delta\omega/2} = \frac{2\Delta\omega}{\pi}\frac{\kappa_{\text{out},b}}{\kappa_b}\frac{\kappa_{\text{out},a}}{(\kappa_{\text{out},a}+\kappa_{\text{loss}})^2}\,, \tag{5.30}$$

where we have substituted the contributions to the total decay rate κ_a from Eq. 5.6. We can see that this result is practically equivalent to that from our initial quick calculation in the Introduction. Above's expression can now be optimised over the decay from the cavity $\kappa_{\text{out},a}$ in order to maximise the number of output photons. We derive Eq. (5.30) and obtain that there is a maximum of stretched photons when it holds that

$$\kappa_{\text{out},a} = \kappa_{\text{loss}}, \tag{5.31}$$

this is, when we balance out the losses of the cavity exactly with the output decay from the cavity. If photons stayed longer in the cavity, losses would be too big, while if they decayed faster to avoid the loss then the bandwidth would not be maximally compressed.

5.2.2 Multi-mode contribution

In this subsection we want to study the effect of unwillingly coupling to neighbouring longitudinal modes. From the single mode contribution, one could get the naive picture that as long as the condition $\kappa_{\text{out},a} = \kappa_{\text{loss}}$ holds, the maximal number of stretched photons would always be obtained. Thus, we could be tempted to make a very big cavity to decrease its free spectral range and thus narrow the photon's bandwidth as much as desired. However, the bigger the cavity, the more likely it will be that the input photons couple to other cavity modes beside the resonant one. This error will effectively reduce the number of stretched photons, and therefore we must find a compromise between the two effects.

In order to study the effect of the rest of the cavity modes we need to consider the full Hamiltonian from Eq. (5.8). One can in principle switch to several rotating frames. The optimal one is that where the Hamiltonian remains time-dependent, such that the adiabatic elimination later on does not return trivial results (Brion et al., 2007). This preferred frame is centered around the driving frequency $\omega'_{a,0}$, which is resonant with the resonant cavity mode $\omega_{a,0}$. That is, a similar rotating frame as in the single mode case, but where

$$\hat{H}_0 = \hbar\omega'_{a,0} \sum_i \hat{a}_i^\dagger \hat{a}_i + \hbar\omega'_{b,0} \hat{b}^\dagger \hat{b}\,, \tag{5.32}$$

instead. By applying Eq. (5.13) to this case we obtain the interaction-picture Hamiltonian

$$\hat{H}' = \hbar \sum_i \Delta_{a,i} \hat{a}_i^\dagger \hat{a}_i + \hbar\Delta_b \hat{b}^\dagger \hat{b} + \hbar \sum_i \left(\tilde{\Omega}_i(t) \hat{a}_i^\dagger \hat{b} + \tilde{\Omega}_i(t)^* \hat{b}^\dagger \hat{a}_i \right) , \tag{5.33}$$

where we have defined the detuning from the rest of the cavity modes as $\Delta_{a,i} \equiv \omega_{a,i} - \omega'_{a,0}$ and the mode-dependent coupling

$$\tilde{\Omega}_i(t) = \Omega(t) e^{i((\omega_{a,i} - \Delta_{a,i}) - (\omega_b - \Delta_b))t}\,. \tag{5.34}$$

We then apply Eqs. 5.5 to obtain a new set of coupled differential equations

$$\begin{aligned} \dot{\hat{a}}_i(t) &= -\left(i\Delta_{a,i} + \frac{\kappa_{a,i}}{2}\right)\hat{a}_i(t) - i\tilde{\Omega}_i(t)\hat{b}(t), \quad \hat{a}_{\text{out},i}(t) = \sqrt{\kappa_{\text{out},a,i}}\hat{a}_i(t) \\ \dot{\hat{b}}(t) &= -\left(i\Delta_b + \frac{\kappa_b}{2}\right)\hat{b}(t) - i\sum_j \tilde{\Omega}_j^*(t)\hat{a}_j(t) + \sqrt{\kappa_{\text{out},b}}\hat{b}_{in}(t), \quad \hat{b}_{in}(t) = \sqrt{\kappa_{\text{out},b}}\hat{b}(t)\,. \end{aligned} \tag{5.35}$$

Performing the same adiabatic elimination as in the single mode case leads still to a set of equations very difficult to solve analytically. In past attempts to solve the system, our next approach was to adiabatically eliminate the modes $\hat{a}_i$ as well, assuming that they also decay fast from the cavity since they are not resonant. This approximation also led to a complicated set of coupled differential equations. Alternatively we directly substituted our solution from the single mode case (Eq. 5.21), but this approach also proved to lead to a difficult problem to solve analytically. We thus make a stronger approximation: we perform perturbation theory to first order, neglecting the interaction between cavity modes through the input mode $\hat{b}(t)$. However, the system is unfortunately still difficult to solve only by requiring this condition, so we finally do both perturbation theory and the adiabatic elimination of the other cavity modes, assuming that the $\hat{a}_{i\neq 0}(t)$ modes are slow varying compared to the resonant mode and not interacting among themselves such that

$$\begin{aligned} \dot{\hat{a}}_i(t) &= -\left(i\Delta_{a,i} + \frac{\kappa_{a,i}}{2}\right)\hat{a}_i(t) - i\tilde{\Omega}_i(t)\hat{b}(t) = 0 \\ \Rightarrow \quad \hat{a}_{i\neq 0}(t) &\simeq -i\frac{\tilde{\Omega}_i(t)\hat{b}(t)}{\left(i\Delta_{a,i} + \frac{\kappa_{a,i}}{2}\right)} = -i\frac{\tilde{\Omega}_i(t)\hat{b}_{in}(t)}{\left(i\Delta_{a,i} + \frac{\kappa_{a,i}}{2}\right)\sqrt{\kappa_{\text{out},b}}}\,, \end{aligned} \tag{5.36}$$

where we have again assumed that there is no output field from the input mode $\hat{b}_{\text{out}}(t) = 0$. Since we are solving the problem of maximising the output of stretched photons to first order, we use the solution for the pulse $\Omega(t)$ that we found for the single-mode case. We are nevertheless aware that this is not necessarily the optimal solution when all the modes at considered at once (see Eq. (5.11)). For the single mode case, we had chosen the wavefunction $\psi(t', T)$ such that the overlap with the input mode $\hat{b}_{in}$ was maximal (see Eq. (5.27)). That is, we require $\psi(t', T)$ to satisfy

$$\psi(t, T) = \hat{b}^{\dagger}_{in}(t) = \sqrt{\frac{2\kappa_{QD}}{1 - e^{-2\kappa_{QD}(T - t_0)}}}e^{-\kappa_{QD}(t - t_0)}\,, \tag{5.37}$$

where for the input mode we assume an exponential decay from the quantum dot single-photon source at a rate κ_{QD}, normalised over the total pulse length T such that $\int_{t_0}^{T} dt|\hat{b}_{in}(t)|^2 = 1$. We then insert above's equation into Eq. (5.36). For simplicity, we decide to drive the $\hat{b}(t)$ input field resonantly, such that $\Delta_b = 0$ and that therefore the coupling pulse is real, i.e. $\tilde{\Omega}_i(t) \in \Re$. This imposes the following condition over the complex phase ϕ_i, defined as $\Omega_i(t) \equiv |\Omega(t)|e^{i\phi_i(t)}$

$$\tilde{\Omega}_i(t) \in \Re \iff \phi_i(t) = -(\omega_{a,i} - \Delta_{a,i} - \omega_{b,0})t\,. \tag{5.38}$$

This phase was in fact expected to be cancelled out since we moved to the specified rotating frame before.

Moving forward, by means of the single-mode pulse solution found in Eq. (5.26) we find that

$$|\Omega(t)| = \sqrt{2\kappa_{QD}}\sqrt{\frac{\Delta_b^2 + (\frac{\kappa_b}{2})^2}{\kappa_b}}\frac{e^{-\kappa_{QD}(t-t_0)}}{\sqrt{1-e^{-2\kappa_{QD}(t-t_0)}}}\,, \tag{5.39}$$

and since $\hat{a}_{\text{out},MM}(t) = \sum_i \sqrt{\kappa_{\text{out},a,i}} f(k_i, z)\hat{a}_i(t)$ it follows that

$$\hat{a}_{\text{out},MM}(t) = -i\sum_i \sqrt{\frac{\kappa_{\text{out},a,i}}{\kappa_{\text{out},b}\kappa_b}}\frac{f(k_i,z)}{i\Delta_{a,i} + \frac{\kappa_{a,i}}{2}} \cdot \\ 2\kappa_{QD}\sqrt{\Delta_b^2 + (\frac{\kappa_b}{2})^2}\frac{e^{-2\kappa_{QD}(t-t_0)}}{\sqrt{(1-e^{-2\kappa_{QD}(T-t_0)})(1-e^{-2\kappa_{QD}(t-t_0)})}}\,, \tag{5.40}$$

where we have taken into account that each of the cavity modes contribute to the total output cavity mode $\hat{a}_{\text{out}}(t)$ weighted by its own decay rate from the cavity $\kappa_{\text{out},a,i}$ and a spatial dependent function $f(k_i, z)$ that describe the spatial dependence of each of the modes. It is expected to depend on the positioning of the NL, as well as its finite size. We will describe the functions $f(k_i, z)$ more in detail in the following sections. For now, we proceed to calculate the Fourier transform of the output mode $\hat{a}_{\text{out}}(t)$. For this, we need to calculate the following integral:

$$\frac{1}{\sqrt{2\pi}}\int_{t_0}^{\infty} dt e^{+i\omega t}\frac{e^{-2\kappa_{QD}(t-t_0)}}{\sqrt{1-e^{-2\kappa_{QD}(t-t_0)}}} = \frac{1}{2\kappa_{QD}\sqrt{2\pi}}e^{-i\omega t_0}B\left(1 - \frac{i\omega}{2\kappa_{QD}}, \frac{1}{2}\right)\,, \tag{5.41}$$

where $B(a,b) = \int_0^1 t^{a-1}(1-t)^{b-1}dt$ is the Beta function, yielding

$$\hat{a}_{\text{out},MM}(\omega) = \\ = -i\sum_i \sqrt{\frac{\kappa_{\text{out},a,i}}{2\pi\kappa_{\text{out},b}\kappa_b}}\frac{f(k_i,z)}{i\Delta_{a,i} + \frac{\kappa_{a,i}}{2}}\sqrt{\Delta_b^2 + (\frac{\kappa_b}{2})^2}\frac{e^{i\omega t_0}}{\sqrt{1-e^{-2\kappa_{QD}(T-t_0)}}}B\left(1 - \frac{i\omega}{2\kappa_{QD}}, \frac{1}{2}\right)\,. \tag{5.42}$$

We can then finally obtain the number of photons that coupled to the off-resonant cavity modes as

$$\int_{-\Delta\omega/2}^{\Delta\omega/2} d\omega \hat{a}^\dagger_{\text{out},MM}(\omega)\hat{a}_{\text{out},MM}(\omega) \simeq \\ \simeq \frac{2\Delta\omega}{\pi}\frac{\kappa_{\text{out},a}\left(\Delta_b^2 + (\frac{\kappa_b}{2})^2\right)}{\kappa_{\text{out},b}\kappa_b\left(1-e^{-2\kappa_{QD}(T-t_0)}\right)}\sum_{ij}\frac{f(k_i,z)f^*(k_j,z)}{(\frac{\kappa_a}{2} + i\Delta_{a,i})(\frac{\kappa_a}{2} - i\Delta_{a,j})}\,, \tag{5.43}$$

where we have assumed that all the modes decay out of the cavity at the same rate $\kappa_{\mathrm{out},a,i} \approx \kappa_{\mathrm{out},a}$ and where we have calculated that, for a small bandwidth $\Delta\omega$,

$$\begin{aligned}\int_{-\Delta\omega/2}^{\Delta\omega/2} d\omega B\left(1-\frac{i\omega}{2\kappa_{QD}},\frac{1}{2}\right)B\left(1+\frac{i\omega}{2\kappa_{QD}},\frac{1}{2}\right) = \\ = \int_{-\Delta\omega/2}^{\Delta\omega/2} d\omega \frac{2\pi\kappa_{QD}\omega \coth\frac{\pi\omega}{2\kappa_{QD}}}{\kappa_{QD}^2+\omega^2} \\ \simeq \int_{-\Delta\omega/2}^{\Delta\omega/2} d\omega \left(4+\frac{(\pi^2-12)\omega^2}{3\kappa_{QD}^2}\right) \approx 4\Delta\omega\,.\end{aligned} \tag{5.44}$$

We would like to remark that equation (5.43) depends on the spatial functions $f(k_i, z)$. Thus if chosen appropriately, the position of the non-linearity can provide a useful phase to further optimise the output, as we will analyse later on.

5.2.3 Crossed terms

We finally obtain the crossed terms from Eq. (5.11) by using the results obtained in Eqs. (5.28) and (5.42), obtaining

$$\begin{aligned}\int_{-\Delta\omega/2}^{\Delta\omega/2} d\omega \hat{a}^{\dagger}_{\mathrm{out},SM}(\omega)\hat{a}_{\mathrm{out},MM}(\omega) = \\ = \frac{\kappa_{\mathrm{out},a}}{2\pi\kappa_b}\frac{\sqrt{\Delta_b^2+(\frac{\kappa_b}{2})^2}}{\sqrt{1-e^{-2\kappa_{QD}(T-t_0)}}}\sum_i \frac{f(k_i,z)}{i\Delta_{a,i}+\frac{\kappa_{a,i}}{2}}\int_{-\Delta\omega/2}^{\Delta\omega/2} d\omega \frac{B\left(1-\frac{i\omega}{2\kappa_{QD}},\frac{1}{2}\right)}{\kappa_a+i\omega}\,.\end{aligned} \tag{5.45}$$

We approximate to first order in ω the integral above by considering a small bandwidth $\Delta\omega$, as in the previous subsections, yielding

$$\frac{B\left(1-\frac{i\omega}{2\kappa_{QD}},\frac{1}{2}\right)}{\kappa_a+i\omega} \simeq \frac{2}{\kappa_a} - \frac{2i\left(\kappa_{QD}+\kappa_a(\log 2-1)\right)}{\kappa_a^2\kappa_{QD}}\omega\,. \tag{5.46}$$

With above's result we can then calculate the number of photons corresponding to the crossed terms as

$$\begin{aligned}\int_{-\Delta\omega/2}^{\Delta\omega/2} d\omega \hat{a}^{\dagger}_{\mathrm{out},SM}(\omega)\hat{a}_{\mathrm{out},MM}(\omega) = \\ = \frac{\Delta\omega}{\pi}\frac{\kappa_{\mathrm{out},a}}{(\kappa_{\mathrm{out},a}+\kappa_{\mathrm{loss}})\,\kappa_b}\frac{\sqrt{\Delta_b^2+(\frac{\kappa_b}{2})^2}}{\sqrt{1-e^{-2\kappa_{QD}(T-t_0)}}}\sum_i \frac{f(k_i,z)}{\frac{\kappa_a}{2}+i\Delta_{a,i}}\,,\end{aligned} \tag{5.47}$$

where we have substituted the total decay $\kappa_a = \kappa_{\mathrm{out},a} + \kappa_{\mathrm{loss}}$.

5.2.4 Total contribution

We can now calculate the total number of photons inserting the results from Eqs. (5.43), (5.30), and (5.47) into Eq. (5.11)

$$\begin{aligned} N = \frac{2\Delta\omega}{\pi}\frac{\kappa_{\text{out},b}}{\kappa_{\text{out},b}+\kappa_{\text{loss}}}\frac{\kappa_{\text{out},a}}{(\kappa_{\text{out},a}+\kappa_{\text{loss}})^2}\cdot \\ \left[1+\frac{(\kappa_{\text{out},a}+\kappa_{\text{loss}})^2}{\kappa_{\text{out},b}^2}\frac{\Delta_b^2+(\frac{\kappa_b}{2})^2}{1-e^{-2\kappa_{QD}(T-t_0)}}|\alpha(z,\kappa_a)|^2\right. \\ \left. +\Re\left\{\frac{\kappa_{\text{out},a}+\kappa_{\text{loss}}}{\kappa_{\text{out},b}}\sqrt{\frac{\Delta_b^2+(\frac{\kappa_b}{2})^2}{1-e^{-2\kappa_{QD}(T-t_0)}}}\alpha(z,\kappa_a)\right\}\right], \end{aligned} \tag{5.48}$$

where we have defined the spatial-dependent functions $\alpha(z,\kappa_a)$ as

$$\alpha(z,\kappa_a) \equiv \sum_n \frac{f(k_n,z)}{\frac{\kappa_a}{2}+i\Delta_{a,n}}\,. \tag{5.49}$$

We can see how the coupling to the other cavity modes $\omega_{a,i}$ modifies the function to be optimised such that it is no longer ideal to choose $\kappa_{\text{out},a}=\kappa_{\text{loss}}$, as we saw in the single-mode case.

To proceed from here we need to calculate the sums in Eq. (5.49). For this, the spatial functions $f(k_i,z)$ need to be determined. We can calculate them from the consequent reflections of the electric field inside of the cavity and obtaining the corresponding field that is emitted to one of the sides (see Fig. x):

$$E_{x,R}(\boldsymbol{r}) = |E_{x,R}|\left(e^{ik_n(L-z)}+r_1r_2e^{ik_n((L-z)+2L)}+(r_1r_2)^2e^{ik_n((L-z)+4L)}+...\right)\,, \tag{5.50}$$

where R is the reflection coefficient of the cavity. We can then solve the geometric series and obtain the Green's function

$$G(k_n,z) = \frac{e^{ik_n(L-z)}}{1-r_1r_2e^{i2k_nL}}\,. \tag{5.51}$$

We then substitute that $\Delta_{a,i}=\frac{n\pi c}{L}$ after calculating the poles of the Green's function, obtaining

$$f(k_n,z) = e^{i\Delta_{a,i}(L-z)/c}\,. \tag{5.52}$$

Thus the sum yields

$$
\begin{aligned}
\alpha(z,\kappa_a) &= \sum_{\substack{m=-\infty\\ m\neq 0}}^{\infty} \frac{e^{i\Delta_{a,i}(L-z)/c}}{\frac{\kappa_a}{2}+i\Delta_{a,i}} = \sum_{\substack{m=-\infty\\ m\neq 0}}^{\infty} \frac{e^{im\pi(1-z/L)}}{\frac{\kappa_a}{2}+i\frac{m\pi c}{L}} = \\
&\simeq \frac{\kappa_a}{2}\frac{L^2}{\pi^2 c^2}\sum_{\substack{m=-\infty\\ m\neq 0}}^{\infty} \frac{e^{im\pi(1-z/L)}}{m^2} - i\frac{L}{\pi c}\sum_{\substack{m=-\infty\\ m\neq 0}}^{\infty} \frac{e^{im\pi(1-z/L)}}{m} \\
&= \frac{\kappa_a}{2}\frac{L^2}{\pi^2 c^2}\left(\mathrm{Li}_2(e^{-i\pi(1-z/L)}) + \mathrm{Li}_2(e^{+i\pi(1-z/L)})\right) \\
&\qquad\qquad - i\frac{L}{\pi c}\left(\log(1-e^{-i\pi(1-z/L)}) - \log(1-e^{+i\pi(1-z/L)})\right)\,,
\end{aligned}
\tag{5.53}
$$

where the function $Li_2(z)$ is the polylogarithm function $Li_n(z)$ with $n=2$, where we have used the approximation

$$
\frac{1}{\frac{\kappa_a}{2}+i\Delta_{a,i}} \simeq \frac{\frac{\kappa_a}{2}-i\Delta_{a,i}}{\Delta_{a,i}^2}\,, \tag{5.54}
$$

which is valid since the decay rate should be much smaller than that of the input pulse, as in $\kappa_a \ll 1/T$, if we want to stretch the photon's pulse-length. Furthermore, since we want to couple as little as possible to the "bad" modes, also $1/T \ll |\omega_i|$ must hold for $i \neq 0$. Thus $\kappa_a \ll |\omega_i|$ and therefore we can approximate $\alpha(z,\kappa_a)$ to first order in κ_a as shown above.

5.3 Conclusion and next steps

As stated in the beginning of the chapter, these are preliminary results from a project that is still ongoing. Therefore, unfortunately we can not have all the figures and final conclusions just yet. The following steps in the analysis would be to explicitly show how the stretching factor η is penalised due to the multimode contributions, both with the analytical approximation derived above and with a fully numerical computation, which is on its way. We hope nevertheless to have shown the potential of this implementation for closing the bandwidth mismatch between different qubit platforms. In fact, the set-up is not limited to the coupling between single-photons and optomechanical quantum memories and is applicable to other systems that suffer from the same challenge.

Final remarks

In the last chapter we collect the conclusions from the different projects presented in the thesis, as well as a road map for future steps of the studies in the outlook section.

Conclusion

In this thesis we have presented different studies that in different ways contribute to developing a secure and global quantum network. Each of the projects has aimed to face one of the challenges that this longer term goal imposes. We have started by investigating in depth different quantum information sources, in particular, quantum-dot single-photon sources and an on-demand path-entanglement generation source. Then we proceeded to analyse how to secure the quantum network where these sources would be implemented by means of Device-Independent Quantum Key Distribution (DIQKD), relating their experimental imperfections to the violation of Bell's inequality and the obtainment of a positive secret key-rate between the emitter and receiver nodes. Finally we proposed a new method to overcome the bandwidth matching problem between single-photons and long-coherence quantum memories such optomechanical membranes.

Specifically, in Chapter 1 we modelled the visibility, purity, and efficiency of the single-photon sources, finding a clear correlation between them and the loophole-free violation of Bell's inequality by means of the discussed heralded scheme. While the HOM visibility and $g^{(2)}$ of current quantum-dot single-photon sources are proficient enough to comply with the requirements for the violation, the required local efficiency ($\eta \approx 90\%$ for realistic values of visibility and purity) is still far from that present in current experiments nowadays. We thus wanted to investigate next if this threshold would relax when using non-maximally entangled states instead of the maximally entangled used in Chapter 1. We implemented this hypothesis in the analysis from Chapter 4, together with a security proof to go beyond loophole-free violation of Bell's inequality and perform a full DIQKD protocol secure against general attacks instead. The experimental conditions for performing DIQKD with single-photon sources were indeed improved with respect to previous studies thanks to basing our security proof on tighter bounds for a potential eavesdropper's information (Brown et al., 2021), and the local efficiency required for a loophole-free violation of Bell's inequality was lowered with respect to the thresholds found in Chapter 1.

Regarding the relation between HOM visibility and purity of the single-photon sources introduced in Chapter 2, we found that the usual expression $V_{HOM} = 1-2g^{(2)}$ adopted by the experimental community is generally incorrect. Instead we presented a detailed analysis where we show that the slope F that governs the relation $V_{HOM} = 1 - Fg^{(2)}$ can in fact take values $F \in [1, 3]$ for single-photon sources depending on the degree of indistinguishability of the photons generated. With this result we therefore encourage the community to fully characterise the HOM visibility of their sources and use the correct value of F accordingly. In Chapter 3, on the other hand, we presented the theoretical analysis of the entanglement quality of the path-entanglement generation sources experimentally implemented by Østfeldt et al. (2022). We found these entanglement sources to be highly promising after modelling their main experimental imperfections: fine-structure splitting, timing jitter and imperfect waveguide directional-coupling.

Finally, in Chapter 5 we presented the single-photon stretcher as a proposal to close the bandwidth mismatch between single-photons an narrow-bandwidth quantum memories. Although still work in progress, we showed how placing a non-linear crystal at a specific position in an optical cavity and driving it with an optimised pulse shape can ideally efficiently elongate the pulse length of the single photon up to a factor equal to the finesse of the cavity.

Outlook

The projects presented in this thesis opened the door to pursuing some research directions further. In particular, we believe that new heralded schemes can be designed in order to further improve the experimental requirements for the implementation of DIQKD protocols with optical devices. One direction could be to design the optical circuit in a way such that Alice's and Bob's measurement are also heralded, in a QND-measurement fashion. This could maybe be implemented by means of extra entangled states shared between Alice and Bob, for example by introducing the path-entangled states described in the thesis. Another option could be to use the spin degree of freedom of QDs to encode the entangled state between Alice and Bob. If the spin state can be read-out efficiently with a single-shot measurement, this would solve the issue of the local efficiency requirements. An alternative is to study schemes that use quantum repeaters and quantum memories (Sangouard et al., 2007). As a shorter term solution, if the required local efficiencies are not yet complied, one could study the possibilities of one-sided DIQKD schemes with single-photon sources (Branciard et al., 2012). Alternately, understanding if Measurement-Device-Independent QKD schemes greatly simplify the local efficiency requirements would depend upon a new analysis to correlate the imperfections with the achievable key rate, since the map between fully DIQKD results to MDIQKD is not completely trivial. On a different note, we believe it could be on the interest of the single-photon source community to develop a user-friendly library to perform an accurate analysis of the relation between the HOM visibility and the second-order correlation function, such that it becomes a routinely correction in the experimental implementations.

Appendix A

Appendix to Chapter 1

A.1 Dephasing in single-photon emitters

To evaluate the performance of the protocol we need to evaluate the indistinguishability parameters α_{ij} and β_{ij} (and higher order moments). In this section we calculate these for a particular model of the dephasing, which was also considered in (Kambs et al., 2018). We consider a Hamiltonian that describes the dynamics of the system, containing the field, the emitter and their interaction (Das et al., 2019):

$$\hat{H} = \left(\omega_{eg}^i + \Delta_i + F_i(t)\right) |e_i\rangle \langle e_i| + \int dk \omega_k \hat{a}_k^\dagger \hat{a}_k - \int dk g_k |e_i\rangle \langle g_i| \hat{a}_k e^{ikz_i} + h.c.\,, \quad \text{(A.1)}$$

where ω_{eg}^i is the natural frequency splitting of each emitter, perturbed by a slow frequency drift Δ_i and rapidly varying (e.g. phonon-induced) random fluctuations represented by the uncorrelated force $F_i(t)$. Solving the time evolution of the system through Schrödinger's equation with a suitable wavefunction ansatz (Das et al., 2019) allows us to find the mode functions $f_i(t)$ appearing in Eq. (1.3):

$$f_i(t, t_0) = \sqrt{\gamma} e^{-\frac{\gamma}{2}(t-t_0)} e^{-i\left(\Delta_i(t-t_0)+\int_{t_0}^{t} F_i(t')dt'\right)} \equiv \sqrt{\gamma} e^{-\frac{\gamma}{2}(t-t_0)} e^{-i(\Delta_i(t-t_0)+\phi_i(t,t_0))}\,, \quad \text{(A.2)}$$

where we account for the spontaneous decay (with spontaneous emission rate γ) and dephasing of the emitter through the random phase ϕ_i. We assume that the uncorrelated force $F_i(t)$ satisfies $\langle F_i(t)\rangle = 0$ and (Bylander, J. et al., 2003)

$$\langle F_i(t)F_j(t')\rangle = 2\gamma_d \delta_{ij}\delta(t-t')\,, \quad \text{(A.3)}$$

where γ_d is the pure dephasing rate. This model for dephasing is equivalent to the standard density matrix description where a decay rate γ_d is added to the off-diagonal elements of the density matrix and has e.g. been shown to provide a good description for phonon induced dephasing in quantum dots (Tighineanu et al., 2018; Muljarov et al., 2004).

We can now use the above model above to evaluate the desired correlation functions. From Eq. (1.4) we have

$$\left\langle |\alpha_{ij}|^2 \right\rangle = \int_{t_0}^{\infty}\int_{t_0}^{\infty} dtdt' \left\langle f_i^*(t,t_0) f_j^*(t',t_0) f_i(t',t_0) f_j(t,t_0) \right\rangle . \tag{A.4}$$

Substituting Eq. (A.3) into A.4, assuming that the energy level in the quantum dot evolves slowly enough in time such that $\Delta_i = \Delta_j$, we find

$$\left\langle |\alpha_{ij}|^2 \right\rangle = \iint_{t_0}^{\infty} dtdt' \gamma^2 \exp\{-\gamma(t+t'-2t_0)\} \left\langle \exp\{-i\left(\phi_i(t') + \phi_j(t) - \phi_i(t) - \phi_j(t')\right)\}\right\rangle . \tag{A.5}$$

Since white noise is necessarily Gaussian, we have a Gaussian distribution for $\phi_i(t)$, leading to

$$\left\langle |\alpha_{ij}|^2 \right\rangle = \\ = \iint_{t_0}^{\infty} dtdt' \gamma^2 \exp\{-\gamma(t+t'-2t_0)\} \exp\left\{\left\langle -\frac{\left\langle (\phi_i(t') + \phi_j(t) - \phi_i(t) - \phi_j(t'))^2 \right\rangle}{2} \right\rangle\right\} . \tag{A.6}$$

Applying Eq. (A.3) the expectation value in the exponent yields

$$\left\langle (\phi_i(t') + \phi_j(t) - \phi_i(t) - \phi_j(t'))^2 \right\rangle = 4\gamma_d |t'-t| , \tag{A.7}$$

finally after substituting in Eq. (A.6), this leads to

$$\left\langle |\alpha_{ij}|^2 \right\rangle = \frac{\gamma}{\gamma + 2\gamma_d} . \tag{A.8}$$

In a similar fashion, one can obtain higher order terms, that are relevant for the three and four photon contributions:

$$\langle \alpha_{ij}\alpha_{ik}\alpha_{jk} \rangle = \frac{\gamma^2}{(\gamma+\gamma_d)(\gamma+2\gamma_d)}, \quad \langle \alpha_{ij}\alpha_{kl}\alpha_{ik}\alpha_{jl} \rangle = \frac{\gamma^3 (3\gamma + 5\gamma_d)}{(\gamma+\gamma_d)(\gamma+2\gamma_d)^2(3\gamma+2\gamma_d)} , \tag{A.9}$$

where $i \neq j \neq k$. Note that $\langle \alpha_{ij}\alpha_{kl} \rangle = \langle \alpha_{ij} \rangle \langle \alpha_{kl} \rangle$ for $i, j \neq k, l$, since the noise is uncorrelated.

On the other hand, when the photons are generated at different stations, we can no longer assume that the energy splitting is zero during each run of the experiment. The slow drift implies a splitting $\Delta_{ij} \equiv \Delta_j - \Delta_i \neq 0$, yielding the following expectation value of the indistinguishability parameter β_{ij}:

$$\left\langle |\beta_{ij}|^2 \right\rangle = \iint_{t_0}^{\infty} dtdt' \gamma^2 \exp\{-\gamma(t+t'-2t_0)\} \exp\{-i\Delta_{ij}(t-t') - 2\gamma_d |t'-t|\} , \tag{A.10}$$

where we have again calculated the expectation value as in Eq. (A.7). Solving these integrals gives us

$$\left\langle |\beta_{ij}|^2 \right\rangle = \frac{\gamma\left(\gamma+2\gamma_d\right)}{\left(\gamma+2\gamma_d\right)^2+\Delta_{ij}^2} \,. \tag{A.11}$$

Similarly we can obtain the higher order terms that are needed for calculating the necessary correlations:

$$\langle \alpha_{ij}\beta_{ik}\beta_{jk}\rangle = \frac{\gamma^2\left(12\left(\gamma+\gamma_d\right)^2\left(\gamma+2\gamma_d\right)^2+\left(3\gamma^2+6\gamma\gamma_d+4\gamma_d^2\right)\Delta^2\right)}{\left(3\left(\gamma+\gamma_d\right)\left(\gamma+2\gamma_d\right)\left(4\left(\gamma+\gamma_d\right)^2+\Delta^2\right)\left(\left(\gamma+2\gamma_d\right)^2+\Delta^2\right)\right)},$$

$$\begin{aligned}\langle \alpha_{ij}\alpha_{kl}\beta_{ik}\beta_{jl}\rangle = \frac{\gamma}{3\gamma+2\gamma_d}\Bigg(&-\frac{8\gamma_d\left(\gamma+\gamma_d\right)\left(2\gamma+\gamma_d\right)}{\left(\gamma+2\gamma_d\right)\left(4\left(\gamma+\gamma_d\right)^2+\Delta^2\right)}+\frac{3\gamma^2+6\gamma\gamma_d+2\gamma_d^2}{\left(\gamma+2\gamma_d\right)^2+\Delta^2}\\ &+\frac{2\gamma_d^2\left(3\gamma+2\gamma_d\right)^2}{\left(\gamma+2\gamma_d\right)^2\left(\left(3\gamma+2\gamma_d\right)^2+\Delta^2\right)}\Bigg).\end{aligned} \tag{A.12}$$

Note that as we assume that all photons are generated by only two quantum dots, there is in fact only one value of the detuning. Therefore we can reduce it to a single value Δ regardless of the considered index.

To apply the above results we need to average over the slow variations of Δ. We assume a Gaussian distribution centered around $\Delta = 0$ with standard deviation σ described by $P(\Delta) = 1/\left(\sqrt{2\pi}\sigma\right)\exp\left\{\frac{-\Delta^2}{2\sigma^2}\right\}$. When we take the average we obtain:

$$\begin{aligned}\left\langle |\beta_{ij}|^2 \right\rangle &= \sqrt{\frac{\pi}{2}}\frac{\gamma}{\sigma}e^{\frac{(\gamma+2\gamma_d)^2}{2\sigma^2}}\mathrm{erfc}\left(\frac{\gamma+2\gamma_d}{\sqrt{2}\sigma}\right),\\ \langle \alpha_{ij}\beta_{ik}\beta_{jk}\rangle &= \sqrt{\frac{\pi}{2}}\frac{\gamma}{3\sigma(\gamma+\gamma_d)(\gamma+2\gamma_d)}\left(e^{\frac{(\gamma+2\gamma_d)^2}{2\sigma^2}}(\gamma+2\gamma_d)(3\gamma+2\gamma_d)\mathrm{erfc}\left(\frac{\gamma+2\gamma_d}{\sqrt{2}\sigma}\right)\right.\\ &\qquad\left.-4e^{\frac{2(\gamma+\gamma_d)^2}{\sigma^2}}\gamma_d(\gamma+\gamma_d)\mathrm{erfc}\left(\frac{\sqrt{2}(\gamma+\gamma_d)}{\sigma}\right)\right),\\ \langle \alpha_{ij}\alpha_{kl}\beta_{ik}\beta_{jl}\rangle &= \sqrt{\frac{\pi}{2}}\frac{\gamma}{\sigma(3\gamma+2\gamma_d)(\gamma+2\gamma_d)^2}\left(2e^{\frac{(3\gamma+2\gamma_d)^2}{2\sigma^2}}\gamma_d^2(3\gamma+2\gamma_d)\mathrm{erfc}\left(\frac{3\gamma+2\gamma_d}{\sqrt{2}\sigma}\right)+\right.\\ &\qquad e^{\frac{(\gamma+2\gamma_d)^2}{2\sigma^2}}(\gamma+2\gamma_d)(3\gamma^2+6\gamma\gamma_d+2\gamma_d^2)\mathrm{erfc}\left(\frac{\gamma+2\gamma_d}{\sqrt{2}\sigma}\right)\\ &\qquad\left.-4e^{\frac{2(\gamma+\gamma_d)^2}{\sigma^2}}\gamma_d(2\gamma+\gamma_d)(\gamma+2\gamma_d)\mathrm{erfc}\left(\frac{\sqrt{2}(\gamma+\gamma_d)}{\sigma}\right)\right).\end{aligned} \tag{A.13}$$

Although exact, the above expressions give trouble numerically when $\sigma \to 0$. Therefore, an asymptotic expansion of the complementary error functions has been used for $\sigma < 0.1$. We express it up to third non-vanishing order

$$\mathrm{erfc}(x) \simeq \frac{1}{\sqrt{\pi}} e^{-x^2} \left(\frac{1}{x} - \frac{1}{2x^3} + \frac{3}{4x^5} \right) . \tag{A.14}$$

For instance, $\langle |\beta_{ij}|^2 \rangle$ becomes

$$\left\langle |\beta_{ij}|^2 \right\rangle \simeq \frac{\gamma}{\gamma + 2\gamma_d} \left(1 - \frac{\sigma^2}{(\gamma + 2\gamma_d)^2} + \frac{3\sigma^4}{(\gamma + 2\gamma_d)^4} \right) , \tag{A.15}$$

which shows that $\langle |\beta_{ij}|^2 \rangle (\sigma = 0) = \langle |\alpha_{ij}|^2 \rangle$, as expected. In a similar way, we calculate the expansion for higher order of the indistinguishability parameters.

A.2 Photon operator transformations

In this appendix we show explicitly how the optical set up transforms the initial creation operators and give more details of the model we use to describe the different errors mechanisms. From Eqs. (1.4) and 1.12 we obtain the global transformation

$$\hat{a}^\dagger_{s,\varsigma} = \frac{\sqrt{\eta_t T}}{2} \left(i \left(\hat{p}^\dagger_H \pm \hat{p}^\dagger_V \right) + \left(\hat{q}^\dagger_H \pm \hat{q}^\dagger_V \right) \right) + i\sqrt{1-T} \hat{a}^\dagger_\varsigma , \tag{A.16}$$

and similarly for Bob's photons, where $\varsigma \in \{H, V\}$. We now apply Eq. (A.16) to all operators in the initial state of the system $\hat{a}^\dagger_{s,H} \hat{a}^\dagger_{s,V} \hat{b}^\dagger_{s,H} \hat{b}^\dagger_{s,V} |\emptyset\rangle$ and trace out the CHS operators $\hat{p}^\dagger_H$, $\hat{p}^\dagger_V$, $\hat{q}^\dagger_H$ and $\hat{q}^\dagger_V$ to obtain the state shared by Alice and Bob after the heralding. This state, as explained in section 1.2, will depend on the detection pattern at the CHS. If we ignore all imperfections and restrict the state to those events where photons lead to clicks corresponding to opposite polarizations

$$|\psi_{D1D4}\rangle = \frac{\eta_t T (1-T)}{\sqrt{2}} \left| \psi^- \right\rangle = - |\psi_{D2D3}\rangle , \tag{A.17}$$

whereas the state that is created after the patterns D_1D_2 and D_3D_4 is

$$|\psi_{D1D2}\rangle = |\psi_{D3D4}\rangle = \frac{i\eta_t T (1-T)}{\sqrt{2}} \left| \phi^- \right\rangle , \tag{A.18}$$

agreeing with our HOM arguments from section 1.2.

In this work we focus the analysis on the patterns that generate the state $|\psi^-\rangle$ (D_1D_4 and D_2D_3) in order to simplify the presentation of the results. Note that the transmission probability only enters in the prefactor of the unnormalised state. After renormalization to account for the state conditioned on the detection of the photons, the states are independent of the transmission efficiency thanks to the heralding scheme.

The heralding station notifies Alice and Bob when the correct pattern of clicks has been detected. In the ideal scenario these patterns guarantee that the protocol succeeded in generating the desired state. To evaluate the performance under non-ideal condition, however, we need to consider the error mechanisms described in the previous section. To do this we start by describing the transformation of the mode operators when a photon is lost:

$$\hat{a}_i^\dagger \to \sqrt{\eta_{j,i}}\hat{a}_i^\dagger + \sqrt{1-\eta_{j,i}}\hat{c}_{j,i}^\dagger \,, \tag{A.19}$$

where $\hat{c}_{j,i}^\dagger$ creates a photon that escapes the set up. The index $j \in \{1, 2, t\}$ indicates where the loss happened following the notation from Fig. 1.3. Applying this transformation to each segment of the setup leads us to the loss operator $\hat{L}_i^\dagger$:

$$\hat{L}_i^\dagger \equiv \sqrt{1-\eta_{1,i}}\hat{c}_{1,i}^\dagger + i\sqrt{\eta_{1,i}(1-\eta_{2,i})(1-T)}\hat{c}_{2,i}^\dagger + \sqrt{\eta_{1,i}(1-\eta_t)T}\hat{c}_{t,i}^\dagger \,. \tag{A.20}$$

The operator directly provides the total probability for the photon to escape the set-up $\left\langle \hat{L}_i\hat{L}_i^\dagger \right\rangle = 1-\eta_{1,i}\eta_{2,i}(1-T)-\eta_{1,i}\eta_t T$. Note that $\left\langle \hat{L}_i\hat{L}_j^\dagger \right\rangle_{i\neq j} = 0$ and $\left\langle \hat{L}_i\hat{L}_j\hat{L}_k^\dagger\hat{L}_l^\dagger \right\rangle_{i\neq k, j\neq l} = 0$ expressing that lost photons do not interfere. By means of Eqs. (A.19) and A.20 we can obtain the global transformation in the main text (B.7).

Finally, we detail the action of the consecutive QWP and HWP on the creation operators $\hat{a}_{H,1}^\dagger$, $\hat{a}_{V,2}^\dagger$, $\hat{b}_{H,3}^\dagger$ and $\hat{b}_{V,4}^\dagger$, represented by the Jones matrices. They are described by the unitary operations (James et al., 2001):

$$\hat{U}_{QWP}(\theta) = \frac{1}{\sqrt{2}}\begin{pmatrix} i-\cos(2\theta) & \sin(2\theta) \\ \sin(2\theta) & i+\cos(2\theta)\end{pmatrix}, \quad \hat{U}_{HWP}(\phi) = \begin{pmatrix} \cos(2\phi) & -\sin(2\phi) \\ -\sin(2\phi) & -\cos(2\phi)\end{pmatrix}. \tag{A.21}$$

The total transformation is thus $\hat{U}_{tot}(\theta,\phi) = \hat{U}_{HWP}(\phi)\hat{U}_{QWP}(\theta)$.

A.3 Conditioning on the correct detection pattern

In this appendix we explicitly show the expectation values of the CHS operators $\hat{O}_i$ up to three-photon detections as a function of the indistinguishability parameters α_{ij} and β_{ij}. Selecting only the combinations of operators that lead to a correct event, that is, D_1D_4 and D_2D_3 and applying Eqs. (1.4) and (1.4), we obtain:

$$\begin{aligned}\left\langle \hat{O}_1\hat{O}_3\hat{O}_1^\dagger\hat{O}_3^\dagger \right\rangle_{D1D4,D2D3} = \frac{1}{2}\langle((\hat{p}_{H,3}\hat{q}_{H,1} + \hat{p}_{V,3}\hat{q}_{H,1}) - (\hat{p}_{H,1}\hat{q}_{H,3} + \hat{p}_{V,1}\hat{q}_{H,3}))\cdot \\ ((\hat{p}_{H,3}^\dagger\hat{q}_{H,1}^\dagger + \hat{p}_{V,3}^\dagger\hat{q}_{H,1}^\dagger) - (\hat{p}_{H,1}^\dagger\hat{q}_{H,3}^\dagger + \hat{p}_{V,1}^\dagger\hat{q}_{H,3}^\dagger)) = 1-|\beta_{13}|^2 \,.\end{aligned} \tag{A.22}$$

Similarly, for the other combinations:

$$\begin{aligned}
&\left\langle \hat{O}_1\hat{O}_4\hat{O}_1^\dagger\hat{O}_4^\dagger\right\rangle_{D1D4,D2D3} = 2t(1-t)1+|\beta_{14}|^2, \quad \left\langle \hat{O}_2\hat{O}_3\hat{O}_2^\dagger\hat{O}_3^\dagger\right\rangle_{D1D4,D2D3} = 1+|\beta_{23}|^2,\\
&\left\langle \hat{O}_2\hat{O}_4\hat{O}_2^\dagger\hat{O}_4^\dagger\right\rangle_{D1D4,D2D3} = 1-|\beta_{24}|^2, \quad \left\langle \hat{O}_1\hat{O}_2\hat{O}_1^\dagger\hat{O}_2^\dagger\right\rangle_{D1D4,D2D3} = 1-|\alpha_{12}|^2,\\
&\left\langle \hat{O}_3\hat{O}_4\hat{O}_3^\dagger\hat{O}_4^\dagger\right\rangle_{D1D4,D2D3} = 1-|\alpha_{34}|^2, \quad \left\langle \hat{O}_1\hat{O}_4\hat{O}_2^\dagger\hat{O}_3^\dagger\right\rangle_{D1D4,D2D3} = -\alpha_{12}\alpha_{34}-\beta_{13}\beta_{24},\\
&\left\langle \hat{O}_1\hat{O}_3\hat{O}_2^\dagger\hat{O}_4^\dagger\right\rangle_{D1D4,D2D3} = -\alpha_{12}\alpha_{34}+\beta_{14}\beta_{23}\,.
\end{aligned} \tag{A.23}$$

It can be easily checked that any other combination of CHS operators has vanishing expectation value. If no conditioning on the detection pattern is done, the sum of the expectation values are independent of the indistinguishability of the photons and equal 4, reflecting that with the current normalization this is proportional to the product of the number of photons at each side. Note that in the limit of completely indistinguishable photons ($\alpha_{12}=\alpha_{34}=1$), $\left\langle \hat{O}_1\hat{O}_2\hat{O}_1^\dagger\hat{O}_2^\dagger\right\rangle_{D1D4,D2D3}$ and $\left\langle \hat{O}_3\hat{O}_4\hat{O}_3^\dagger\hat{O}_4^\dagger\right\rangle_{D1D4,D2D3}$ vanish, meaning that we never have a successful detection event with two photons from the same station. As explained in Sec. 1.2, this occurs because of the HOM effect, since two photons from from the same station will bunch together after the half-wave plate ($\hat{a}_{H,1}^\dagger\hat{a}_{V,2}^\dagger \to \hat{a}_H'^{\dagger 2} - \hat{a}_V'^{\dagger 2}$), and therefore no D_1D_4 or D_2D_3 clicks can ever happen. Finally, note that the expectation values in Eq. (A.23) correspond to the generalised matrix elements of the density matrix in Eq. (1.22).

In a similar manner, we can calculate the expectation values for the occurrence of three photons at the CHS. We only keep those terms that correspond to combinations of clicks perceived as correct by the CHS, D_1D_4 and D_2D_3, due to the detectors not being photon-number resolving. For instance, a term such $\hat{p}_{H,1}^\dagger\hat{q}_{V,3}^\dagger\hat{q}_{V,4}^\dagger$ is taken into consideration, while $\hat{p}_{H,1}^\dagger\hat{p}_{V,3}^\dagger\hat{q}_{V,4}^\dagger$ is not. Applying once more Eqs. (1.4) and (1.4) we obtain

$$\begin{aligned}
\left\langle \hat{O}_1\hat{O}_3\hat{O}_4\hat{O}_1^\dagger\hat{O}_3^\dagger\hat{O}_4^\dagger\right\rangle_{D1D4,D2D3} &= \frac{1}{2}\left(3-|\alpha_{34}|^2-|\beta_{13}|^2+3|\beta_{14}|^2-2\alpha_{34}\beta_{13}\beta_{14}\right),\\
\left\langle \hat{O}_2\hat{O}_3\hat{O}_4\hat{O}_2^\dagger\hat{O}_3^\dagger\hat{O}_4^\dagger\right\rangle_{D1D4,D2D3} &= \frac{1}{2}\left(3-|\alpha_{34}|^2+3|\beta_{23}|^2-|\beta_{24}|^2-2\alpha_{34}\beta_{23}\beta_{24}\right),\\
\left\langle \hat{O}_3\hat{O}_1\hat{O}_2\hat{O}_3^\dagger\hat{O}_1^\dagger\hat{O}_2^\dagger\right\rangle_{D1D4,D2D3} &= \frac{1}{2}\left(3-|\alpha_{12}|^2-|\beta_{13}|^2+3|\beta_{23}|^2-2\alpha_{12}\beta_{13}\beta_{23}\right),\\
\left\langle \hat{O}_4\hat{O}_1\hat{O}_2\hat{O}_4^\dagger\hat{O}_1^\dagger\hat{O}_2^\dagger\right\rangle_{D1D4,D2D3} &= \frac{1}{2}\left(3-|\alpha_{12}|^2+3|\beta_{14}|^2-|\beta_{24}|^2-2\alpha_{12}\beta_{14}\beta_{24}\right),
\end{aligned} \tag{A.24}$$

where again any other combination of three CHS operators has an expectation value equal zero.

A.4 Probability events P_{ijkl}

In this section we include Table A.1, where we detail the contribution of all 4 and 5-photon events.

Event probability	CHS	Alice	Bob	Lost photons
P_{2110}	AB	A	B	∅
P_{2200}	BB	AA	∅	∅
P_{2020}	AA	∅	BB	∅
P_{2101}	AB	A	∅	B
	BB	A	∅	A
P_{2011}	AB	∅	B	A
	AA	∅	B	B
P_{2002}	AB	∅	∅	AB
	AA	∅	∅	BB
	BB	∅	∅	AA
P_{3100}	ABB	A	∅	∅
P_{3010}	AAB	∅	B	∅
P_{3001}	ABB	∅	∅	A
	AAB	∅	∅	B
P_{2111}	AB	A	B	A
	AA	A	B	B
P_{2210}	AB	AA	B	∅
P_{2120}	AA	A	BB	∅
P_{2201}	AB	AA	∅	B
	BB	AA	∅	A
P_{2021}	AA	∅	BB	A
P_{2102}	AB	A	∅	AB
	AA	A	∅	BB
	BB	A	∅	AA
P_{2012}	AB	∅	B	AA
	AA	∅	B	AB
P_{2300}	BB	AAA	∅	∅
P_{2030}	AA	BBB	∅	∅
P_{2003}	AB	∅	∅	AAB
	AA	∅	∅	ABB
	BB	∅	∅	AAA
P_{3110}	AAB	A	B	∅
P_{3101}	AAB	A	∅	B
	ABB	A	∅	A
P_{3011}	AAA	∅	B	B
	AAB	∅	B	A
P_{3200}	ABB	AA	∅	∅
P_{3020}	AAA	∅	BB	∅
P_{3002}	AAA	∅	∅	BB
	AAB	∅	∅	AB
	ABB	∅	∅	AA

Table A.1: 4-photon and 5-photon events that lead to a correct detection pattern at the CHS. A and B indicate where the photons were generated, while the header tells where they were detected.

Appendix B

Appendix to Chapter 4

B.1 Equivalence between the assignment strategy in CHSH and Eberhard's inequality

It is well known that the CHSH inequality has an efficiency threshold of 82.84% (Massar et al., 2002) limited by its incapability of assuming non-detection events. Alternatively, one can think of either assignment strategies (this is, to allocate a determined output if nothing was detected) or consider inequalities such Eberhard (Eberhard, 1993), which accounts for non-detection events and has an efficiency threshold of 66%. There is, however, a common confusion in the literature regarding the efficiency required by a Bell test experiment in order to close the detection loophole. In many cases, as in two of the three loophole-free Bell test from 2015 (Giustina et al., 2015; Shalm et al., 2015), the use of Eberhard is expressed to be advantageous by means of non-maximally entangled states. It can be proved, however, that if CHSH is used together with an assignment strategy, the two inequalities are equivalent. In order to prove it we follow Czechlewski et al. (2018).

Proof. We start by writing Eberhard's inequality (Eberhard, 1993):

$$J \equiv p(0,0|0,0) - p(0,0|1,1) - p(0,1|0,1) - p(1,0|1,0) - p(0,\emptyset|0,1) - p(\emptyset,0|1,0) \leq 0\,. \tag{B.1}$$

Now we calculate the marginal probabilities $p_A(0|0)$ and $p_B(0|0)$, adding the extra terms due to the assignment strategy $\emptyset \to 1$:

$$\begin{aligned} p_A(0|0) &= \sum_b p(0,b|0,y) = p(0,0|0,y) + p(0,1|0,y) + p(0,\emptyset|0,y) \\ p_B(0|0) &= \sum_a p(a,0|x,0) = p(0,0|x,0) + p(1,0|x,0) + p(\emptyset,0|x,0)\,. \end{aligned} \tag{B.2}$$

Furthermore, the marginal probabilities of Alice and Bob are assumed to be independent of each other inputs under the deterministic assumption, thus we conveniently choose

$$\begin{aligned} p_A(0|0) &= \sum_b p(0,b|0,1) = p(0,0|0,1) + p(0,1|0,1) + p(0,\emptyset|0,1) \\ p_B(0|0) &= \sum_a p(a,0|1,0) = p(0,0|1,0) + p(1,0|1,0) + p(\emptyset,0|1,0)\,, \end{aligned} \tag{B.3}$$

and substitute in Eq. B.4, obtaining

$$p(0,0|0,0) - p(0,0|1,1) + p(0,0|1,0) + p(0,0|0,1) - p_A(0|0) - p_B(0|0) \leq 0\,, \tag{B.4}$$

which is known as CH inequality (Clauser et al., 1974). Multiplying the CH inequality by 4, adding 2 on both sides of the inequality and $\pm 2p_A(0|1) \pm 2p_B(0|1)$, we can collect all terms as

$$\sum_{xy}^{1} (-1)^{xy} \Big(4p(0,0|x,y) - 2p_A(0|x) - 2p_B(0|y) + 1 \Big) \leq 2\,, \tag{B.5}$$

and recalling that we have assigned $\emptyset \to 1$, we insert the value of the marginals $p_A(0|x)$ and $p_A(0|y)$, yielding

$$\sum_{xy}^{1} (-1)^{xy} \Big(p(0,0|x,y) - p(0,1|x,y) - p(1,0|x,y) + p(1,1|x,y) \Big) \leq 2\,, \tag{B.6}$$

which corresponds to CHSH inequality. □

B.2 Modelling of real single-photon sources and detectors

The probabilities p_{ijkl} that contribute to the total heralding probability are closely related to those derived in González-Ruiz et al. (2022a), but had to be recalculated. The reason is that the probability contributions were previously obtained by averaging over the states heralded by the detector combinations D_1D_4 and D_2D4 (see Table 4.1), which effectively cancels out the effect of the variable central beam splitter transmittance t on the generated entangled state. In addition, compared to González-Ruiz et al. (2022a) we neglect terms where three photons click simultaneously in an acceptable pattern at the CHS, since their probability of occurring is at least an order of magnitude smaller than the 2-photon events.

The initial state is given by the creation of the single photon product state $\hat{a}^\dagger_{1,H}\hat{a}^\dagger_{2,V}\hat{a}^\dagger_{3,H}\hat{a}^\dagger_{4,V}\,|\emptyset\rangle$. The creation operators $\hat{a}^\dagger_{i,\varsigma}$ are then linearly transformed according to

$$\hat{a}^\dagger_{\varsigma,i} \to \sqrt{\frac{\eta_1\eta_t T}{2}}\hat{O}^\dagger_i + i\sqrt{\eta_l}\hat{a}^\dagger_{\varsigma,i} + \hat{L}^\dagger_i\,, \tag{B.7}$$

and similarly for Bob's operators (González-Ruiz et al., 2022a). After the transformation we can see that a photon can be successfully transmitted to the CHS with a probability proportional to $\eta_t T$ ($\hat{O}_i^\dagger$), remain at the local stations after being reflected at the first beam splitter ($\hat{a}_{i,\varsigma}^\dagger$) or lost ($\hat{L}_i^\dagger$). Thus we can trace out the CHS $\hat{O}_i^\dagger$ and loss operators $\hat{L}_i^\dagger$ and condition on the correct detection pattern to obtain the state shared by the remaining photons. See González-Ruiz et al. (2022a) for details.

In particular, for the correct conditioning of the desired detection pattern we obtain several combinations of CHSH operators expectation values. The following expectation values were added or modified with respect to González-Ruiz et al. (2022a):

$$
\begin{aligned}
&\left\langle \hat{O}_1\hat{O}_2\hat{O}_1^\dagger\hat{O}_2^\dagger \right\rangle = 2t(1-t)(1-|\alpha_{12}|^2), \quad \left\langle \hat{O}_3\hat{O}_4\hat{O}_3^\dagger\hat{O}_4^\dagger \right\rangle = 2t(1-t)(1-|\alpha_{34}|^2),\\
&\left\langle \hat{O}_1\hat{O}_3\hat{O}_1^\dagger\hat{O}_3^\dagger \right\rangle = 1-2t(1-t)(1+|\beta_{13}|^2), \quad \left\langle \hat{O}_1\hat{O}_4\hat{O}_1^\dagger\hat{O}_4^\dagger \right\rangle = 1-2t(1-t)(1-|\beta_{14}|^2),\\
&\left\langle \hat{O}_2\hat{O}_3\hat{O}_2^\dagger\hat{O}_3^\dagger \right\rangle = 1-2t(1-t)(1-|\beta_{23}|^2), \quad \left\langle \hat{O}_2\hat{O}_4\hat{O}_2^\dagger\hat{O}_4^\dagger \right\rangle = 1-2t(1-t)(1+|\beta_{24}|^2),\\
&\left\langle \hat{O}_1\hat{O}_4\hat{O}_2^\dagger\hat{O}_3^\dagger \right\rangle = -\alpha_{12}\alpha_{34} + 2t(1-t)(\alpha_{12}\alpha_{34} - \beta_{13}\beta_{24}),\\
&\left\langle \hat{O}_1\hat{O}_3\hat{O}_2^\dagger\hat{O}_4^\dagger \right\rangle = -\alpha_{12}\alpha_{34} + 2t(1-t)(\alpha_{12}\alpha_{34} + \beta_{14}\beta_{23})\\
&\left\langle \hat{O}_1\hat{O}_3\hat{O}_1^\dagger\hat{O}_4^\dagger \right\rangle = \left\langle \hat{O}_2\hat{O}_3\hat{O}_2^\dagger\hat{O}_4^\dagger \right\rangle = \mp(1-2t)\alpha_{34}\\
&\left\langle \hat{O}_1\hat{O}_4\hat{O}_2^\dagger\hat{O}_4^\dagger \right\rangle = \left\langle \hat{O}_1\hat{O}_3\hat{O}_2^\dagger\hat{O}_3^\dagger \right\rangle = \pm(1-2t)\alpha_{12}\,.
\end{aligned}
\tag{B.8}
$$

Here the plus and minus solutions correspond to the heralding combinations $D1D4$ and $D2D3$ respectively and α_{ij} and β_{ij} (with $i,j = 1,2,3,4$ indicating the source) relate to the HOM visibility of photons generated in the same or opposite station respectively, and the decoherence parameters as

$$
V_\alpha = \overline{|\alpha_{ij}|^2}, \quad V_\beta = \overline{|\beta_{ij}|^2} = \sqrt{\frac{\pi}{2}}\frac{\gamma}{\sigma}e^{\frac{(\gamma+2\gamma_d)^2}{2\sigma^2}}\operatorname{erfc}\left(\frac{\gamma+2\gamma_d}{\sqrt{2}\sigma}\right). \tag{B.9}
$$

For this work, we postselect on the $D2D3$ combination.

With the moments specified above we can evaluate the Bell parameter for any settings. We then optimize the violation of CHSH over the measurement angles and the transmittance t for different values of the noise and visibility (see Figure B.1). Comparing to Figure 6 in González-Ruiz et al. (2022a), we not only lower the local efficiency thresholds, but actually reach the theoretical limit $\eta_l = 66.67\%$ expected for CHSH type inequalities with non-maximally entangled states (Eberhard, 1993; Caprara Vivoli et al., 2015). For completeness we also include the CHSH parameter S as a function of the local efficiency η_l for different values of the second order correlation function $g^{(2)}$ in Fig. B.2, which also show improved efficiency thresholds compared to González-Ruiz et al. (2022a).

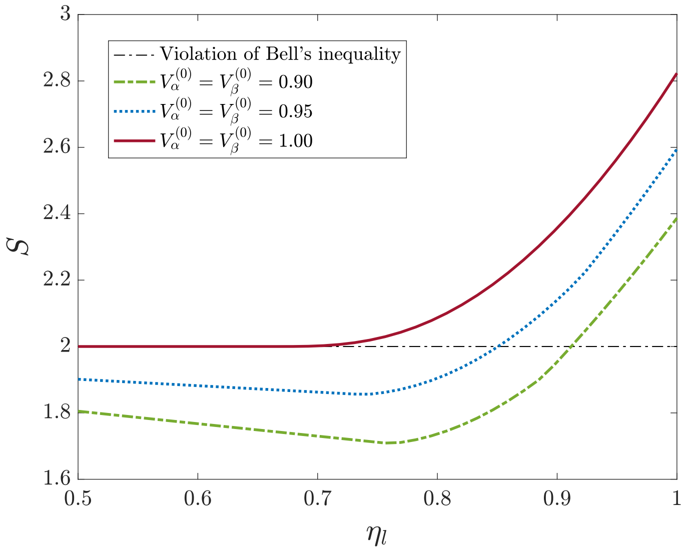


Figure B.1: CHSH parameter S as a function of the local efficiency η_l of Alice and Bob's stations for different HOM visibilities optimized with respect to the transmittance t. To focus on the effect of the local efficiency we consider a situation with a very limited transmission to the CHS ($T = 10^{-3}$ and $\eta_t = 0.1$) and vary the efficiency of the final arm η_2 with $\eta_{1,i} = 1$. We extract a threshold of 66.7% for the efficiency in the perfect visibility case, which agrees with Caprara Vivoli et al. (2015).

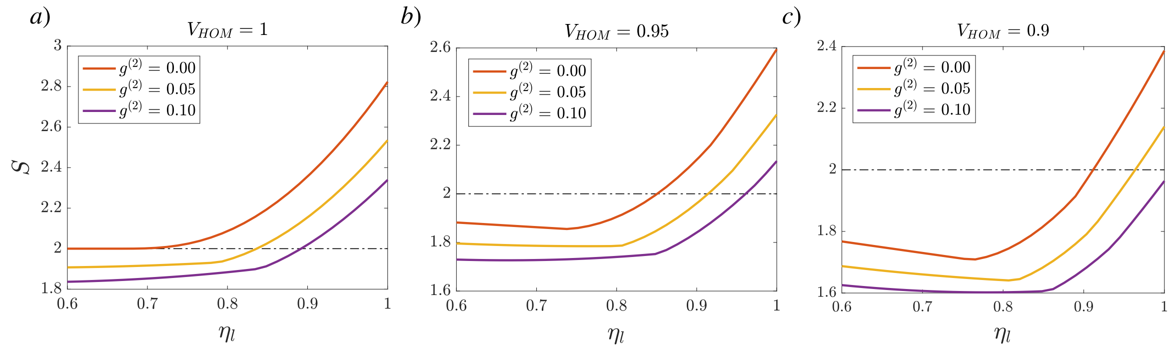


Figure B.2: CHSH parameter S as a function of the local efficiency η_l of Alice and Bob's stations for different purities and HOM visibilities optimized with respect to the transmittance t. We set a low transmittance ($T = 10^{-3}$ and $\eta_t = 0.1$) and vary the efficiency of the final arm η_2 with $\eta_{1,i} = 1$.

B.3 Numerical implementation

In this appendix we provide a description of the numerical implementation for computing the key rate from Eq. (4.8). It consists of three parts:

1. An optimization over the experimental parameters, which has been done by means of the `minimize` function of the `Scipy` package (Virtanen et al., 2020);

2. The generation of the SDP relaxation shown in Eq. (4.8), which has been done by means of the `ncpol2sdpa` package (Wittek, 2015) and minimized using Mosek (ApS, 2022).

3. A parallelization of the process by means of `MPICH` (Message Passing Interface Forum, 2021), such that we can find the SDP relaxation of many non local initial points simultaneously.

Our numerical implementation can be found in González-Ruiz et al. (2022c) and is based on that developed by Peter Brown and coworkers (Brown et al., 2021), using the same approximations as the ones implemented in these references. Let us go, in more detail, through each of the points mentioned above.

B.3.1 Optimization of the experimental parameters

The optimization can be understood as an outside optimization that is done over the SDP relaxation shown in Eq. (4.8). In other words, Eq. (4.8) (adding the relative entropy between Alice and Bob) serves as a function over which we optimize, with the constraints depending on the parameters used in the setup shown in Fig. 4.1 via the probability distribution associated to the configuration. In particular, for the situation where we do not apply noisy preprocessing, we have five parameters over which we optimize, namely $(t, \theta_{A_0}, \theta_{A_1}, \theta_{B_0}, \theta_{B_1}, \theta_{B_2})$. These respectively correspond to the beam splitter transmissivity used in the CHS, the two angles associated to the two possible measurements Alice can perform, and the three angles associated to the three possible measurements Bob can perform. In our numerical implementation, we considered that the A_0 measurement of Alice and the B_2 measurement of Bob are the ones from which Alice and Bob extract the key.

This external optimization has been done using the Nelder-Mead algorithm (Nelder et al., 1965), which is a local optimization method that is particularly suitable for constrained parameters. Concretely, the constraints we impose are $t \in [0, 1]$ and $\theta_{A_i}, \theta_{B_j} \in [0, 2\pi]$. However, the main drawback of this method is that it is local, which implies that (i) it depends on an initial guess; (ii) we can fall into local minima that happen to provide significantly different values for our figure of merit. Thus, it is fundamental for these local methods to generate a big number of instances that are relevant to the problem. In our case, we generated random points satisfying the previous constraints, and filtered them by checking whether the probability they give rise to belongs to the 2222 local polytope. This allow us to fix the parameters

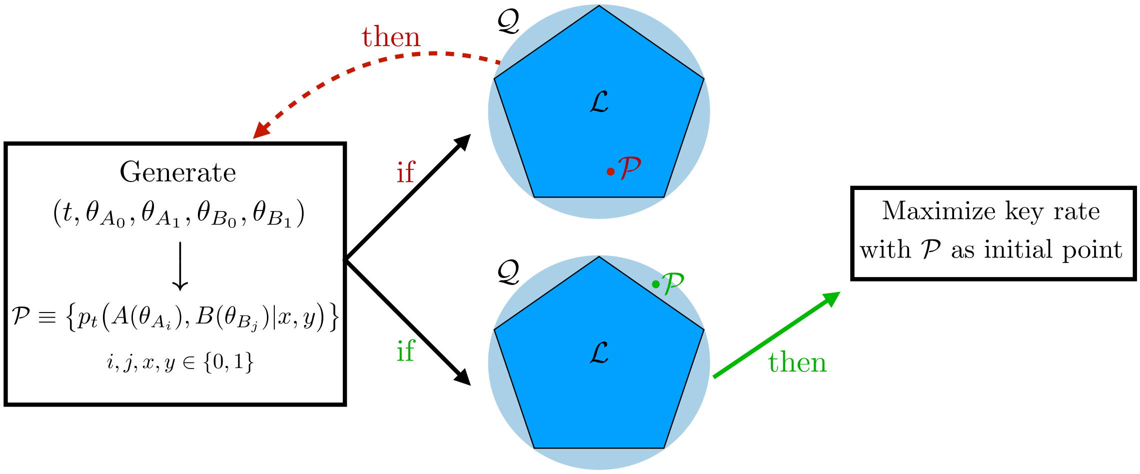


Figure B.3: Schematic representation of our numerical implementation. We first randomly generate a point satisfying a set of conditions imposed by the physical implementation, and compute the associated probability distribution $\mathcal{P}$. Then, we check whether the generated point is within the local set $\mathcal{L}$ or not. If it is, then we generate another point. Otherwise, we use it for running the SDP and maximize the key rate.

$(t, \theta_{A_i}, \theta_{B_j})$, with $i = 0, 1$, while θ_{B_2} remains random. A pictorial representation of this numerical implementation is shown in Fig. B.3.

Each of these nonlocal points are then used as starting points for the local optimization method. The next step is to optimize over the SDP to evaluate the key rate for a given non-local point.

B.3.2 SDP relaxation

It is important to note that the expression we use in Eq. (4.8) is a SDP relaxation to the exact expression considered in Theorem 2.11 of (Brown et al., 2021), based on the Navascués-Pironio-Acín (NPA) hierarchy (Navascués et al., 2007; Navascués et al., 2008). Furthermore, in our numerical implementation, we restrict ourselves to the second level of the hierarchy such that we consider only up to second order moments in our certificate. However, we introduce some extra third order moments, in particular terms of the form ABZ and $AZ^{\dagger}Z$ (where the Z are the Eve operators appearing in Eq. (4.8)).

The SDP relaxation shown in Eq. (4.8) depends on m, which is the maximum number of terms we consider when expanding the integrals that are defined in the quantum relative entropy (for more details, see Theorem 2.11 in Ref. (Brown et al., 2021)). Obviously, in the limit $m \to \infty$ we recover the exact definition of the integral terms, and therefore obtain better bounds (see Fig. (B.4)).

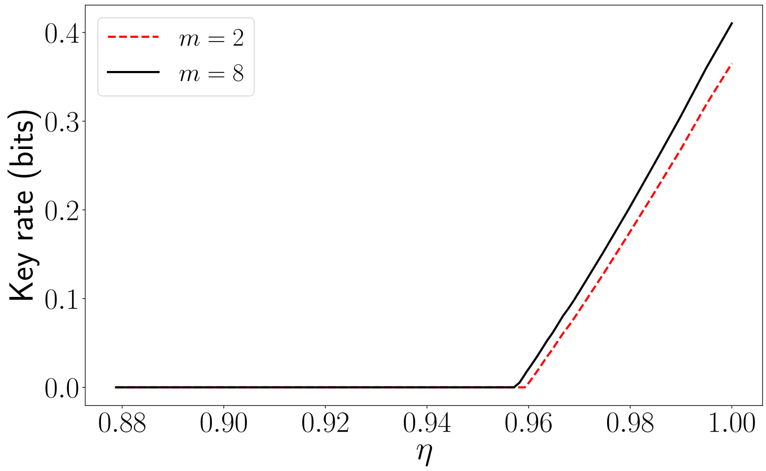


Figure B.4: Key rate for $V = 0.95$ computed with two different values of m: $m = 2$ (red dashed curve) and $m = 8$ (black solid curve). As we can see, increasing the value of m for fixed experimental parameters, leads to better bounds on the relative entropy between Alice and Eve, which translates into higher key rates.

B.3.3 Parallelization

Once we have obtained a certain number of points outside the local set $\mathcal{L}$ that satisfy the conditions of our implementation and have created the SDP relaxation problem, we optimize the measurement angles such that the key rate is maximized. This optimization problem is computationally hard, since it needs to perform the SDP relaxation with each evaluation of the optimization function.

We create a parallelized approach in which the non-local points are optimized in parallel with a MPI standard (Message Passing Interface Forum, 2021). Note that increasing values of m lead to more terms in our SDP relaxation and thus more computation time is needed. In order to get useful results in a reasonable amount of time, we set $m = 2$ for each of the optimizations. By doing this, we filter all those initially generated nonlocal points that clearly lead to bad (negative) values of the key rate. With this we thus obtain a set of *good* points, which can then be evaluated with a bigger value of m ($m = 8$), leading to the plots we show in the main text.

Bibliography

Acín, A., N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani (June 2007). “Device-Independent Security of Quantum Cryptography against Collective Attacks”. In: *Physical Review Letters* 98.23, p. 230501. DOI: 10.1103/PhysRevLett.98.230501 (cit. on pp. 68, 74).

Aghaee, M. et al. (Nov. 2022). *InAs-Al Hybrid Devices Passing the Topological Gap Protocol.* DOI: 10.48550/arXiv.2207.02472. arXiv: 2207.02472 [cond-mat] (cit. on p. 3).

Aharonovich, I., D. Englund, and M. Toth (2016). “Solid-State Single-Photon Emitters”. In: *Nature Photonics* 10.10, pp. 631–641 (cit. on p. 37).

Akopian, N., N. H. Lindner, E. Poem, Y. Berlatzky, J. Avron, D. Gershoni, B. D. Gerardot, and P. M. Petroff (Apr. 2006). “Entangled Photon Pairs from Semiconductor Quantum Dots”. In: *Physical Review Letters* 96.13, p. 130501. DOI: 10.1103/PhysRevLett.96.130501 (cit. on pp. 6, 49, 61).

Andersen, A. L. (2019). “Quantum Key Distribution and Entanglement Distribution with Satellite Links”. MA thesis. University of Copenhagen (cit. on p. 7).

ApS, M. (2022). *MOSEK Optimizer API for Python 9.3.20* (cit. on p. 115).

Arcari, M., I. Söllner, A. Javadi, S. Lindskov Hansen, S. Mahmoodian, J. Liu, H. Thyrrestrup, E. H. Lee, J. D. Song, S. Stobbe, and P. Lodahl (Aug. 2014). “Near-Unity Coupling Efficiency of a Quantum Emitter to a Photonic Crystal Waveguide”. In: *Physical Review Letters* 113.9, p. 093603. DOI: 10.1103/PhysRevLett.113.093603 (cit. on p. 22).

Arnon-Friedman, R., R. Renner, and T. Vidick (2019). “Simple and Tight Device-Independent Security Proofs”. In: *SIAM Journal on Computing* 48.1, pp. 181–225. DOI: 10.1137/18M1174726. eprint: https://doi.org/10.1137/18M1174726 (cit. on p. 68).

Arute, F. et al. (Oct. 2019). “Quantum Supremacy Using a Programmable Superconducting Processor”. In: *Nature* 574.7779, pp. 505–510. DOI: 10.1038/s41586-019-1666-5 (cit. on pp. 1, 3).

Aspuru-Guzik, A. and P. Walther (2012). “Photonic Quantum Simulators”. In: *Nature physics* 8.4, pp. 285–291 (cit. on p. 37).

Babinec, T. M., B. J. M. Hausmann, M. Khan, Y. Zhang, J. R. Maze, P. R. Hemmer, and M. Lončar (Mar. 2010). “A Diamond Nanowire Single-Photon Source”. In: *Nature Nanotechnology* 5.3, pp. 195–199. DOI: 10.1038/nnano.2010.6 (cit. on p. 4).

Bartolucci, S., P. Birchall, H. Bombin, H. Cable, C. Dawson, M. Gimeno-Segovia, E. Johnston, K. Kieling, N. Nickerson, M. Pant, F. Pastawski, T. Rudolph, and C. Sparrow (Jan. 2021). *Fusion-Based Quantum Computation.* DOI: 10.48550/arXiv.2101.09310. arXiv: 2101.09310 [quant-ph] (cit. on p. 49).

Bell, J. S. (Nov. 1964). “On the Einstein Podolsky Rosen Paradox”. In: *Physics Physique Fizika* 1.3, pp. 195–200. DOI: 10.1103/PhysicsPhysiqueFizika.1.195 (cit. on pp. 10, 11).

Bellovin, S. M. (July 2011). “Frank Miller: Inventor of the One-Time Pad”. In: *Cryptologia* 35.3, pp. 203–222. DOI: 10.1080/01611194.2011.583711 (cit. on p. 9).

Bennett, C. H. and G. Brassard (1984). “Quantum Cryptography: Public Key Distribution and Coin Tossing”. In: *Theoretical Computer Science*. Theoretical Aspects of Quantum Cryptography – Celebrating 30 Years of BB84 560, pp. 7–11. DOI: 10.1016/j.tcs.2014.05.025 (cit. on pp. 9, 67).

Bennett, C. H., G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters (Mar. 1993). "Teleporting an Unknown Quantum State via Dual Classical and Einstein-Podolsky-Rosen Channels". In: *Physical Review Letters* 70.13, pp. 1895–1899. DOI: 10.1103/PhysRevLett.70.1895 (cit. on p. 7).

Benson, O., C. Santori, M. Pelton, and Y. Yamamoto (Mar. 2000). "Regulated and Entangled Photons from a Single Quantum Dot". In: *Physical Review Letters* 84.11, pp. 2513–2516. DOI: 10.1103/PhysRevLett.84.2513 (cit. on pp. 6, 49).

Bjerlin, J., E. M. González-Ruiz, and A. S. Sørensen (2023). "Two Photon Correlations for a Quantum-Dot Single Photon Source." In preparation (cit. on pp. i, iii, 14, 24, 37–39).

Boaron, A., G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussières, M.-J. Li, D. Nolan, A. Martin, and H. Zbinden (Nov. 2018). "Secure Quantum Key Distribution over 421 Km of Optical Fiber". In: *Physical Review Letters* 121.19, p. 190502. DOI: 10.1103/PhysRevLett.121.190502 (cit. on p. 9).

Borregaard, J., H. Pichler, T. Schröder, M. D. Lukin, P. Lodahl, and A. S. Sørensen (June 2020). "One-Way Quantum Repeater Based on Near-Deterministic Photon-Emitter Interfaces". In: *Physical Review X* 10.2, p. 021071. DOI: 10.1103/PhysRevX.10.021071 (cit. on p. 7).

Bose, S., P. L. Knight, M. B. Plenio, and V. Vedral (Dec. 1999). "Proposal for Teleportation of an Atomic State via Cavity Decay". In: *Physical Review Letters* 83.24, pp. 5158–5161. DOI: 10.1103/PhysRevLett.83.5158 (cit. on p. 6).

Branciard, C., E. G. Cavalcanti, S. P. Walborn, V. Scarani, and H. M. Wiseman (Jan. 2012). "One-Sided Device-Independent Quantum Key Distribution: Security, Feasibility, and the Connection with Steering". In: *Physical Review A* 85.1, p. 010301. DOI: 10.1103/PhysRevA.85.010301 (cit. on p. 100).

Brańczyk, A. M. (Oct. 2017). *Hong-Ou-Mandel Interference*. DOI: 10.48550/arXiv.1711.00080. arXiv: 1711.00080 [quant-ph] (cit. on pp. 21, 40).

Briegel, H. J., D. E. Browne, W. Dür, R. Raussendorf, and M. Van den Nest (Jan. 2009). "Measurement-Based Quantum Computation". In: *Nature Physics* 5.1, pp. 19–26. DOI: 10.1038/nphys1157 (cit. on p. 49).

Brion, E., L. H. Pedersen, and K. Mølmer (Jan. 2007). "Adiabatic Elimination in a Lambda System". In: *Journal of Physics A: Mathematical and Theoretical* 40.5, p. 1033. DOI: 10.1088/1751-8113/40/5/011 (cit. on p. 93).

Brown, P., H. Fawzi, and O. Fawzi (June 2021). *Device-Independent Lower Bounds on the Conditional von Neumann Entropy*. DOI: 10.48550/arXiv.2106.13692. arXiv: 2106.13692 [quant-ph] (cit. on pp. 13, 69, 74–76, 83, 99, 115, 116).

Brown, R. H. and R.Q. Twiss (1954). "LXXIV. A New Type of Interferometer for Use in Radio Astronomy". In: *The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science* 45.366, pp. 663–682. DOI: 10.1080/14786440708520475. eprint: https://doi.org/10.1080/14786440708520475 (cit. on p. 49).

Bylander, J., Robert-Philip, I., and Abram, I. (2003). "Interference and Correlation of Two Independent Photons". In: *The European Physical Journal D: Atomic, Molecular, Optical and Plasma Physics* 22.2, pp. 295–301. DOI: 10.1140/epjd/e2002-00236-6 (cit. on p. 103).

Calsamiglia, J. and N. Lütkenhaus (Jan. 2001). "Maximum Efficiency of a Linear-Optical Bell-state Analyzer". In: *Applied Physics B* 72.1, pp. 67–71. DOI: 10.1007/s003400000484 (cit. on pp. 6, 19).

Candelon, F., J.-F. Bobier, M. Courtaux, and G. Nahas (Aug. 2022). *Can Europe Catch Up with the US (and China) in Quantum Computing?* Tech. rep. BCG Henderson Institute (cit. on p. 1).

Cao, M., F. Hoffet, S. Qiu, A. S. Sheremet, and J. Laurat (Oct. 2020). "Efficient Reversible Entanglement Transfer between Light and Quantum Memories". In: *Optica* 7.10, pp. 1440–1444. DOI: 10.1364/OPTICA.400695 (cit. on p. 35).

Caprara Vivoli, V., P. Sekatski, J.-D. Bancal, C. C. W. Lim, B. G. Christensen, A. Martin, R. T. Thew, H. Zbinden, N. Gisin, and N. Sangouard (Jan. 2015). "Challenging Preconceptions about Bell Tests with Photon Pairs". In: *Physical Review A: Atomic, Molecular, and Optical Physics* 91.1, p. 012107. DOI: 10.1103/PhysRevA.91.012107 (cit. on pp. 113, 114).

Chan, M. L., Z. Aqua, A. Tiranov, B. Dayan, P. Lodahl, and A. S. Sørensen (June 2022). "Quantum State Transfer between a Frequency-Encoded Photonic Qubit and a Quantum-Dot Spin in a Nanophotonic Waveguide". In: *Physical Review A* 105.6, p. 062445. DOI: 10.1103/PhysRevA.105.062445 (cit. on p. 3).

Cirac, J. I. and P. Zoller (May 1995). "Quantum Computations with Cold Trapped Ions". In: *Physical Review Letters* 74.20, pp. 4091–4094. DOI: 10.1103/PhysRevLett.74.4091 (cit. on p. 3).

Cirel'son, B. S. (Mar. 1980). "Quantum Generalizations of Bell's Inequality". In: *Letters in Mathematical Physics* 4.2, pp. 93–100. DOI: 10.1007/BF00417500 (cit. on p. 11).

Clauser, J. F. and M. A. Horne (July 1974). "Experimental Consequences of Objective Local Theories". In: *Physical Review D: Particles and Fields* 10.2, pp. 526–535. DOI: 10.1103/PhysRevD.10.526 (cit. on p. 112).

Clauser, J. F., M. A. Horne, A. Shimony, and R. A. Holt (Oct. 1969). "Proposed Experiment to Test Local Hidden-Variable Theories". In: *Physical Review Letters* 23.15, pp. 880–884. DOI: 10.1103/PhysRevLett.23.880 (cit. on pp. 10, 26, 68, 74).

Czechlewski, M. and M. Pawłowski (June 2018). "Influence of the Choice of Postprocessing Method on Bell Inequalities". In: *Physical Review A: Atomic, Molecular, and Optical Physics* 97.6, p. 062123. DOI: 10.1103/PhysRevA.97.062123 (cit. on p. 111).

Da Lio, B., C. Faurby, X. Zhou, M. L. Chan, R. Uppu, H. Thyrrestrup, S. Scholz, A. D. Wieck, A. Ludwig, P. Lodahl, and L. Midolo (2022). "A Pure and Indistinguishable Single-Photon Source at Telecommunication Wavelength". In: *Advanced Quantum Technologies* 5.5, p. 2200006. DOI: 10.1002/qute.202200006 (cit. on pp. 7, 86).

Daley, A. J., I. Bloch, C. Kokail, S. Flannigan, N. Pearson, M. Troyer, and P. Zoller (July 2022). "Practical Quantum Advantage in Quantum Simulation". In: *Nature* 607.7920, pp. 667–676. DOI: 10.1038/s41586-022-04940-6 (cit. on p. 1).

Das, S., L. Zhai, M. Čepulskovskis, A. Javadi, S. Mahmoodian, P. Lodahl, and A. S. Sørensen (2019). *A Wave-Function Ansatz Method for Calculating Field Correlations and Its Application to the Study of Spectral Filtering and Quantum Dynamics of Multi-Emitter Systems*. arXiv: 1912.08303 [quant-ph] (cit. on pp. 38, 54, 55, 103).

Devetak, I. and A. Winter (Jan. 2005). "Distillation of Secret Key and Entanglement from Quantum States". In: *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences* 461.2053, pp. 207–235. DOI: 10.1098/rspa.2004.1372 (cit. on pp. 12, 74).

Ding, X., Y. He, Z.-C. Duan, N. Gregersen, M.-C. Chen, S. Unsleber, S. Maier, C. Schneider, M. Kamp, S. Höfling, C.-Y. Lu, and J.-W. Pan (Jan. 2016). "On-Demand Single Photons with High Extraction Efficiency and near-Unity Indistinguishability from a Resonantly Driven Quantum Dot in a Micropillar". In: *Physical Review Letters* 116.2, p. 020401. DOI: 10.1103/PhysRevLett.116.020401 (cit. on pp. 30, 34).

Duan, L.-M., M. D. Lukin, J. I. Cirac, and P. Zoller (Nov. 2001). "Long-Distance Quantum Communication with Atomic Ensembles and Linear Optics". In: *Nature* 414.6862, pp. 413–418. DOI: 10.1038/35106500 (cit. on pp. 6, 37).

Dupuis, F., O. Fawzi, and R. Renner (2020). "Entropy Accumulation". In: *Communications in Mathematical Physics* 379.3, pp. 867–913 (cit. on p. 80).

Eberhard, P. H. (Feb. 1993). "Background Level and Counter Efficiencies Required for a Loophole-Free Einstein-Podolsky-Rosen Experiment". In: *Physical Review A: Atomic, Molecular, and Optical Physics* 47.2, R747–R750. DOI: 10.1103/PhysRevA.47.R747 (cit. on pp. 36, 71, 111, 113).

Eisaman, M. D., J. Fan, A. Migdall, and S. V. Polyakov (July 2011). "Invited Review Article: Single-photon Sources and Detectors". In: *Review of Scientific Instruments* 82.7, p. 071101. DOI: 10.1063/1.3610677 (cit. on p. 4).

Ekert, A. K. (Aug. 1991). "Quantum Cryptography Based on Bell's Theorem". In: *Physical Review Letters* 67.6, pp. 661–663. DOI: 10.1103/PhysRevLett.67.661 (cit. on pp. 9, 67).

European Quantum Flagship, Q. (Nov. 2022). *Strategic Research and Industry Agenda*. Tech. rep. The European Quantum Flagship, p. 49 (cit. on p. 1).

Fan, H., K. Matsumoto, and H. Imai (Mar. 2003). "Quantify Entanglement by Concurrence Hierarchy". In: *Journal of Physics A: Mathematical and General* 36.14, pp. 4151–4158. DOI: 10.1088/0305-4470/36/14/316 (cit. on p. 59).

Fan, J. and A. Migdall (Mar. 2007). "A Broadband High Spectral Brightness Fiber-Based Two-Photon Source". In: *Optics Express* 15.6, pp. 2915–2920. DOI: 10.1364/OE.15.002915 (cit. on p. 4).

Farkas, M., M. Balanzó-Juandó, K. Łukanowski, J. Kołodyński, and A. Acín (July 2021). "Bell Nonlocality Is Not Sufficient for the Security of Standard Device-Independent Quantum Key Distribution Protocols". In: *Physical Review Letters* 127.5, p. 050503. DOI: 10.1103/PhysRevLett.127.050503 (cit. on pp. 76, 77).

Fischer, K. A., R. Trivedi, V. Ramasesh, I. Siddiqi, and J. Vučković (May 2018). "Scattering into One-Dimensional Waveguides from a Coherently-Driven Quantum-Optical System". In: *Quantum* 2, p. 69. DOI: 10.22331/q-2018-05-28-69 (cit. on p. 54).

Fognini, A., A. Ahmadi, S. J. Daley, M. E. Reimer, and V. Zwiller (Sept. 2018). "Universal Fine-Structure Eraser for Quantum Dots". In: *Optics Express* 26.19, pp. 24487–24496. DOI: 10.1364/OE.26.024487 (cit. on p. 61).

Fosco-Connect (2023). *Fiber Loss*. https://www.fiberoptics4sale.com/blogs/wave-optics/fiber-loss (cit. on p. 7).

Gisin, N., S. Pironio, and N. Sangouard (Aug. 2010). "Proposal for Implementing Device-Independent Quantum Key Distribution Based on a Heralded Qubit Amplifier". In: *Physical Review Letters* 105.7, p. 070501. DOI: 10.1103/PhysRevLett.105.070501 (cit. on p. 69).

Giustina, M. et al. (Dec. 2015). "Significant-Loophole-Free Test of Bell's Theorem with Entangled Photons". In: *Physical Review Letters* 115.25, p. 250401. DOI: 10.1103/PhysRevLett.115.250401 (cit. on pp. 11, 15, 16, 111).

González-Ruiz, E. M. (2018). *Characterisation of GaAs Quantum Dots for Solid-State Entangled Photon Sources*. Project Outside the Course Scope. University of Copenhagen: Niels Bohr Institute, p. 18 (cit. on p. 5).

González-Ruiz, E. M., S. K. Das, P. Lodahl, and A. S. Sørensen (July 2022a). "Violation of Bell's Inequality with Quantum-Dot Single-Photon Sources". In: *Physical Review A* 106.1, p. 012222. DOI: 10.1103/PhysRevA.106.012222 (cit. on pp. i, iii, 14, 15, 38, 69–73, 77, 78, 112, 113).

González-Ruiz, E. M., F. T. Østfeldt, R. Uppu, P. Lodahl, and A. S. Sørensen (Jan. 2023). *Entanglement Properties of a Quantum-Dot Biexciton Cascade in a Chiral Nanophotonic Waveguide*. DOI: 10.48550/arXiv.2301.04444. arXiv: 2301.04444 [quant-ph] (cit. on pp. i, iii, 14, 47).

González-Ruiz, E. M., J. Rivera-Dean, M. F. B. Cenni, A. S. Sørensen, A. Acín, and E. Oudot (Nov. 2022b). *Device Independent Quantum Key Distribution with Realistic Single-Photon Source Implementations*. DOI: 10.48550/arXiv.2211.16472. arXiv: 2211.16472 [quant-ph] (cit. on pp. i, iii, 11, 14, 38, 67).

— (2022c). *Device Independent Quantum Key Distribution with Realistic Single-Photon Source Implementations: Code Repository*. DOI: 10.5281/zenodo.7038040 (cit. on p. 115).

Gorshkov, A. V., A. André, M. D. Lukin, and A. S. Sørensen (Sept. 2007). "Photon Storage in $\ensuremath{\Lambda}$-Type Optically Dense Atomic Media. I. Cavity Model". In: *Physical Review A* 76.3, p. 033804. DOI: 10.1103/PhysRevA.76.033804 (cit. on p. 90).

Gorshkov, A. V., J. Otterbach, M. Fleischhauer, T. Pohl, and M. D. Lukin (Sept. 2011). "Photon-Photon Interactions via Rydberg Blockade". In: *Physical Review Letters* 107.13, p. 133602. DOI: 10.1103/PhysRevLett.107.133602 (cit. on p. 3).

Gour, G., M. M. Wilde, S. Brandsen, and I. J. Geng (Aug. 2022). *Inevitability of Knowing Less than Nothing*. DOI: 10.48550/arXiv.2208.14424. arXiv: 2208.14424 [math-ph, physics:quant-ph] (cit. on p. 12).

Harris, S. E., M. K. Oshman, and R. L. Byer (May 1967). "Observation of Tunable Optical Parametric Fluorescence". In: *Physical Review Letters* 18.18, pp. 732–734. DOI: 10.1103/PhysRevLett.18.732 (cit. on p. 4).

Hendrickx, N. W., W. I. L. Lawrie, L. Petit, A. Sammak, G. Scappucci, and M. Veldhorst (July 2020). "A Single-Hole Spin Qubit". In: *Nature Communications* 11.1, p. 3478. DOI: 10.1038/s41467-020-17211-7 (cit. on p. 3).

Hensen, B. et al. (Oct. 2015). "Loophole-Free Bell Inequality Violation Using Electron Spins Separated by 1.3 Kilometres". In: *Nature* 526.7575, pp. 682–686. DOI: 10.1038/nature15759 (cit. on pp. 11, 15, 16).

Heuck, M., K. Jacobs, and D. R. Englund (Apr. 2020). "Photon-Photon Interactions in Dynamically Coupled Cavities". In: *Physical Review A* 101.4, p. 042322. DOI: 10.1103/PhysRevA.101.042322 (cit. on p. 54).

Ho, M., P. Sekatski, E. Y.-Z. Tan, R. Renner, J.-D. Bancal, and N. Sangouard (June 2020). "Noisy Preprocessing Facilitates a Photonic Realization of Device-Independent Quantum Key Distribution". In: *Physical Review Letters* 124.23, p. 230502. DOI: 10.1103/PhysRevLett.124.230502 (cit. on pp. 74, 75, 83).

Hong, C. K., Z. Y. Ou, and L. Mandel (Nov. 1987). "Measurement of Subpicosecond Time Intervals between Two Photons by Interference". In: *Physical Review Letters* 59.18, pp. 2044–2046. DOI: 10.1103/PhysRevLett.59.2044 (cit. on pp. 18, 38).

Horodecki, R., P. Horodecki, M. Horodecki, and K. Horodecki (June 2009). "Quantum Entanglement". In: *Reviews of Modern Physics* 81.2, pp. 865–942. DOI: 10.1103/RevModPhys.81.865 (cit. on p. 47).

Huber, D., M. Reindl, S. F. Covre da Silva, C. Schimpf, J. Martín-Sánchez, H. Huang, G. Piredda, J. Edlinger, A. Rastelli, and R. Trotta (July 2018). "Strain-Tunable GaAs Quantum Dot: A Nearly Dephasing-Free Source of Entangled Photon Pairs on Demand". In: *Physical Review Letters* 121.3, p. 033902. DOI: 10.1103/PhysRevLett.121.033902 (cit. on pp. 6, 49).

Hummel, T., C. Ouellet-Plamondon, E. Ugur, I. Kulkova, T. Lund-Hansen, M. A. Broome, R. Uppu, and P. Lodahl (2019). "Efficient Demultiplexed Single-Photon Source with a Quantum Dot Coupled to a Nanophotonic Waveguide". In: *Applied Physics Letters* 115.2, p. 021102. DOI: 10.1063/1.5096979. eprint: https://doi.org/10.1063/1.5096979 (cit. on pp. 21, 22).

Huo, Y. H., A. Rastelli, and O. G. Schmidt (Apr. 2013). "Ultra-Small Excitonic Fine Structure Splitting in Highly Symmetric Quantum Dots on GaAs (001) Substrate". In: *Applied Physics Letters* 102.15, p. 152105. DOI: 10.1063/1.4802088 (cit. on p. 61).

James, D. F. V., P. G. Kwiat, W. J. Munro, and A. G. White (Oct. 2001). "Measurement of Qubits". In: *Physical Review A: Atomic, Molecular, and Optical Physics* 64.5, p. 052312. DOI: 10.1103/PhysRevA.64.052312 (cit. on p. 107).

Jozsa, R. and N. Linden (Aug. 2003). "On the Role of Entanglement in Quantum-Computational Speed-Up". In: *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences* 459.2036, pp. 2011–2032. DOI: 10.1098/rspa.2002.1097 (cit. on pp. 6, 47).

Kambs, B. and C. Becher (Nov. 2018). "Limitations on the Indistinguishability of Photons from Remote Solid State Sources". In: *New Journal of Physics* 20.11, p. 115003. DOI: 10.1088/1367-2630/aaea99 (cit. on pp. 22, 103).

Kaniewski, J. (Aug. 2016). "Analytic and Nearly Optimal Self-Testing Bounds for the Clauser-Horne-Shimony-Holt and Mermin Inequalities". In: *Physical Review Letters* 117.7, p. 070402. DOI: 10.1103/PhysRevLett.117.070402 (cit. on p. 68).

Kimble, H. J. (June 2008). "The Quantum Internet". In: *Nature* 453.7198, pp. 1023–1030. DOI: 10.1038/nature07127 (cit. on pp. 1, 37).

Kjaergaard, M., M. E. Schwartz, J. Braumüller, P. Krantz, J. I.-J. Wang, S. Gustavsson, and W. D. Oliver (2020). "Superconducting Qubits: Current State of Play". In: *Annual Review of Condensed Matter Physics* 11.1, pp. 369–395. DOI: 10.1146/annurev-conmatphys-031119-050605. eprint: https://doi.org/10.1146/annurev-conmatphys-031119-050605 (cit. on p. 3).

Knill, E., R. Laflamme, and G. J. Milburn (2001). "A Scheme for Efficient Quantum Computation with Linear Optics". In: *nature* 409.6816, pp. 46–52 (cit. on p. 37).

Kołodyński, J., A. Máttar, P. Skrzypczyk, E. Woodhead, D. Cavalcanti, K. Banaszek, and A. Acín (Apr. 2020). "Device-Independent Quantum Key Distribution with Single-Photon Sources". In: *Quantum* 4, p. 260. DOI: 10.22331/q-2020-04-30-260 (cit. on pp. 16, 17, 35, 36, 69, 70).

Kwiat, P. G. and H. Weinfurter (Oct. 1998). "Embedded Bell-State Analysis". In: *Physical Review A: Atomic, Molecular, and Optical Physics* 58.4, R2623–R2626. DOI: 10.1103/PhysRevA.58.R2623 (cit. on pp. 18, 70).

Larsson, J.-Å. (Oct. 2014). "Loopholes in Bell Inequality Tests of Local Realism". In: *Journal of Physics A: Mathematical and Theoretical* 47.42, p. 424003. DOI: 10.1088/1751-8113/47/42/424003 (cit. on p. 15).

Li, Q., W. Bao, Z. Nie, Y. Xia, Y. Xue, Y. Wang, S. Yang, and X. Zhang (Apr. 2021). "A Non-Unitary Metasurface Enables Continuous Control of Quantum Photon–Photon Interactions from Bosonic to Fermionic". In: *Nature Photonics* 15.4, pp. 267–271. DOI: 10.1038/s41566-021-00762-6 (cit. on p. 3).

LIGO Scientific Collaboration and Virgo Collaboration et al. (Feb. 2016). "Observation of Gravitational Waves from a Binary Black Hole Merger". In: *Physical Review Letters* 116.6, p. 061102. DOI: 10.1103/PhysRevLett.116.061102 (cit. on p. 1).

Liu, J., R. Su, Y. Wei, B. Yao, S. F. C. da Silva, Y. Yu, J. Iles-Smith, K. Srinivasan, A. Rastelli, J. Li, and X. Wang (June 2019). "A Solid-State Source of Strongly Entangled Photon Pairs with High Brightness and Indistinguishability". In: *Nature Nanotechnology* 14.6, pp. 586–593. DOI: 10.1038/s41565-019-0435-9 (cit. on pp. 6, 49).

Liu, W.-Z., M.-H. Li, S. Ragy, S.-R. Zhao, B. Bai, Y. Liu, P. J. Brown, J. Zhang, R. Colbeck, J. Fan, Q. Zhang, and J.-W. Pan (Apr. 2021). "Device-Independent Randomness Expansion against Quantum Side Information". In: *Nature Physics* 17.4, pp. 448–451. DOI: 10.1038/s41567-020-01147-2 (cit. on p. 81).

Lodahl, P., S. Mahmoodian, and S. Stobbe (May 2015). "Interfacing Single Photons and Single Quantum Dots with Photonic Nanostructures". In: *Reviews of Modern Physics* 87.2, pp. 347–400. DOI: 10.1103/RevModPhys.87.347 (cit. on pp. 5, 51, 52).

Lounis, B. and W. E. Moerner (Sept. 2000). "Single Photons on Demand from a Single Molecule at Room Temperature". In: *Nature* 407.6803, pp. 491–493. DOI: 10.1038/35035032 (cit. on p. 4).

Lu, C.-Y. and J.-W. Pan (Dec. 2021). "Quantum-Dot Single-Photon Sources for the Quantum Internet". In: *Nature Nanotechnology* 16.12, pp. 1294–1296. DOI: 10.1038/s41565-021-01033-9 (cit. on pp. 1, 8).

Lugiato, L., F. Prati, and M. Brambilla (2015). *Nonlinear Optical Systems*. Cambridge: Cambridge University Press. DOI: 10.1017/CBO9781107477254 (cit. on p. 90).

Łukanowski, K., M. Balanzó-Juandó, M. Farkas, A. Acín, and J. Kołodyński (Aug. 2022). *Upper Bounds on Key Rates in Device-Independent Quantum Key Distribution Based on Convex-Combination Attacks*. arXiv: 2206.06245 [quant-ph] (cit. on pp. 76, 77).

Lydersen, L., C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov (Oct. 2010). "Hacking Commercial Quantum Cryptography Systems by Tailored Bright Illumination". In: *Nature Photonics* 4.10, pp. 686–689. DOI: 10.1038/nphoton.2010.214 (cit. on p. 68).

Ma, X. and N. Lütkenhaus (Mar. 2012). "Improved Data Post-Processing in Quantum Key Distribution and Application to Loss Thresholds in Device Independent QKD". In: *Quantum Information & Computation* 12.3-4, pp. 203–214 (cit. on pp. 75, 83).

Magde, D. and H. Mahr (May 1967). "Study in Ammonium Dihydrogen Phosphate of Spontaneous Parametric Interaction Tunable from 4400 to 16 000 \AA{}". In: *Physical Review Letters* 18.21, pp. 905–907. DOI: 10.1103/PhysRevLett.18.905 (cit. on p. 4).

Márquez, J., L. Geelhaar, and K. Jacobi (Apr. 2001). "Atomically Resolved Structure of InAs Quantum Dots". In: *Applied Physics Letters* 78.16, pp. 2309–2311. DOI: 10.1063/1.1365101 (cit. on p. 5).

Massar, S., S. Pironio, J. Roland, and B. Gisin (Nov. 2002). "Bell Inequalities Resistant to Detector Inefficiency". In: *Physical Review A: Atomic, Molecular, and Optical Physics* 66.5, p. 052112. DOI: 10.1103/PhysRevA.66.052112 (cit. on pp. 31, 111).

Mayers, D. and A. Yao (Sept. 2004). *Self Testing Quantum Apparatus*. DOI: 10.48550/arXiv.quant-ph/0307205 (cit. on p. 68).

McCuller, L. et al. (Apr. 2020). "Frequency-Dependent Squeezing for Advanced LIGO". In: *Physical Review Letters* 124.17, p. 171102. DOI: 10.1103/PhysRevLett.124.171102 (cit. on p. 1).

McKinsey&Company (Dec. 2021). *Quantum Computing, an Emerging Ecosystem and Industry Use Cases*. Tech. rep. (cit. on p. 1).

Message Passing Interface Forum (June 2021). *MPI: A Message-Passing Interface Standard Version 4.0*. Manual (cit. on pp. 115, 117).

Moore, G. (Jan. 1998). "Cramming More Components Onto Integrated Circuits". In: *Proceedings of the IEEE* 86.1, pp. 82–85. DOI: 10.1109/JPROC.1998.658762 (cit. on p. 2).

Muljarov, E. A. and R. Zimmermann (Nov. 2004). "Dephasing in Quantum Dots: Quadratic Coupling to Acoustic Phonons". In: *Physical Review Letters* 93.23, p. 237401. DOI: 10.1103/PhysRevLett.93.237401 (cit. on pp. 21, 103).

Nadlinger, D. P., P. Drmota, B. C. Nichol, G. Araneda, D. Main, R. Srinivas, D. M. Lucas, C. J. Ballance, K. Ivanov, E. Y.-Z. Tan, P. Sekatski, R. L. Urbanke, R. Renner, N. Sangouard, and J.-D. Bancal (July 2022). "Experimental Quantum Key Distribution Certified by Bell's Theorem". In: *Nature* 607.7920, pp. 682–686. DOI: 10.1038/s41586-022-04941-5 (cit. on pp. 13, 68, 69, 81).

Navascués, M., S. Pironio, and A. Acín (Jan. 2007). "Bounding the Set of Quantum Correlations". In: *Physical Review Letters* 98.1, p. 010401. DOI: 10.1103/PhysRevLett.98.010401 (cit. on pp. 74, 116).

— (July 2008). "A Convergent Hierarchy of Semidefinite Programs Characterizing the Set of Quantum Correlations". In: *New Journal of Physics* 10.7, p. 073013. DOI: 10.1088/1367-2630/10/7/073013 (cit. on pp. 74, 116).

Nelder, J. A. and R. Mead (Jan. 1965). "A Simplex Method for Function Minimization". In: *The Computer Journal* 7.4, pp. 308–313. DOI: 10.1093/comjnl/7.4.308 (cit. on p. 115).

Nielsen, M. A. and I. L. Chuang (Dec. 2010). *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press. DOI: 10.1017/CBO9780511976667 (cit. on p. 12).

O'brien, J. L. (2007). "Optical Quantum Computing". In: *Science (New York, N.Y.)* 318.5856, pp. 1567–1570 (cit. on p. 37).

Ollivier, H, S. Thomas, S. Wein, I. M. de Buy Wenniger, N Coste, J. Loredo, N Somaschi, A Harouri, A Lemaitre, I Sagnes, et al. (2021). "Hong-Ou-Mandel Interference with Imperfect Single Photon Sources". In: *Physical Review Letters* 126.6, p. 063602 (cit. on pp. 24, 38).

Østfeldt, F. T. (Nov. 2020). "Deterministic Single and Multi-Photon Sources with Antum Dots in Planar Nanostructures". PhD thesis. University of Copenhagen (cit. on p. 5).

Østfeldt, F. T., E. M. González-Ruiz, N. Hauff, Y. Wang, A. D. Wieck, A. Ludwig, R. Schott, L. Midolo, A. S. Sørensen, R. Uppu, and P. Lodahl (June 2022). "On-Demand Source of Dual-Rail Photon Pairs Based on Chiral Interaction in a Nanophotonic Waveguide". In: *PRX Quantum* 3.2, p. 020363. DOI: 10.1103/PRXQuantum.3.020363 (cit. on pp. i, iii, 6, 14, 47, 49, 56, 57, 60, 64, 65, 100).

Pedersen, F. T., Y. Wang, C. T. Olesen, S. Scholz, A. D. Wieck, A. Ludwig, M. C. Löbl, R. J. Warburton, L. Midolo, R. Uppu, and P. Lodahl (2020). "Near Transform-Limited Quantum Dot Linewidths in a Broadband Photonic Crystal Waveguide". In: *ACS Photonics* 7.9, pp. 2343–2349. DOI: 10.1021/acsphotonics.0c00758. eprint: https://doi.org/10.1021/acsphotonics.0c00758 (cit. on p. 51).

Pironio, S., A. Acín, N. Brunner, N. Gisin, S. Massar, and V. Scarani (Apr. 2009). "Device-Independent Quantum Key Distribution Secure against Collective Attacks". In: *New Journal of Physics* 11.4, p. 045021. DOI: 10.1088/1367-2630/11/4/045021 (cit. on pp. 9, 12, 15, 16, 30).

Politi, A., J. C. Matthews, M. G. Thompson, and J. L. O'Brien (Nov. 2009). "Integrated Quantum Photonics". In: *IEEE Journal of Selected Topics in Quantum Electronics* 15.6, pp. 1673–1684. DOI: 10.1109/JSTQE.2009.2026060 (cit. on p. 49).

Renner, R. and R. Wolf (June 2022). *Quantum Advantage in Cryptography*. DOI: 10.48550/arXiv.2206.04078. arXiv: 2206.04078 [quant-ph] (cit. on p. 8).

Renou, M.-O., D. Trillo, M. Weilenmann, T. P. Le, A. Tavakoli, N. Gisin, A. Acín, and M. Navascués (Dec. 2021). "Quantum Theory Based on Real Numbers Can Be Experimentally Falsified". In: *Nature* 600.7890, pp. 625–629. DOI: 10.1038/s41586-021-04160-4 (cit. on p. 2).

Ripka, F., H. Kübler, R. Löw, and T. Pfau (Oct. 2018). "A Room-Temperature Single-Photon Source Based on Strongly Interacting Rydberg Atoms". In: *Science* 362.6413, pp. 446–449. DOI: 10.1126/science.aau1949 (cit. on p. 4).

Rivest, R. L., A. Shamir, and L. Adleman (Feb. 1978). "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems". In: *Communications of the ACM* 21.2, pp. 120–126. DOI: 10.1145/359340.359342 (cit. on p. 8).

Rossi, M., D. Mason, J. Chen, Y. Tsaturyan, and A. Schliesser (Nov. 2018). "Measurement-Based Quantum Control of Mechanical Motion". In: *Nature* 563.7729, pp. 53–58. DOI: 10.1038/s41586-018-0643-8 (cit. on pp. 13, 85).

Ruihong, Q. and M. Ying (June 2019). "Research Progress Of Quantum Repeaters". In: *Journal of Physics: Conference Series* 1237.5, p. 052032. DOI: 10.1088/1742-6596/1237/5/052032 (cit. on p. 7).

Sangouard, N., C. Simon, H. de Riedmatten, and N. Gisin (Mar. 2011). "Quantum Repeaters Based on Atomic Ensembles and Linear Optics". In: *Reviews of Modern Physics* 83.1, pp. 33–80. DOI: 10.1103/RevModPhys.83.33 (cit. on pp. 7, 37).

Sangouard, N., C. Simon, J. Minář, H. Zbinden, H. de Riedmatten, and N. Gisin (Nov. 2007). "Long-Distance Entanglement Distribution with Single-Photon Sources". In: *Physical Review A* 76.5, p. 050301. DOI: 10.1103/PhysRevA.76.050301 (cit. on p. 100).

Scarani, V., H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev (Sept. 2009). "The Security of Practical Quantum Key Distribution". In: *Reviews of Modern Physics* 81.3, pp. 1301–1350. DOI: 10.1103/RevModPhys.81.1301 (cit. on p. 67).

Seis, Y., T. Capelle, E. Langman, S. Saarinen, E. Planz, and A. Schliesser (Mar. 2022). "Ground State Cooling of an Ultracoherent Electromechanical System". In: *Nature Communications* 13.1, p. 1507. DOI: 10.1038/s41467-022-29115-9 (cit. on p. 85).

Sekatski, P., J.-D. Bancal, X. Valcarce, E. Y.-Z. Tan, R. Renner, and N. Sangouard (Apr. 2021). "Device-Independent Quantum Key Distribution from Generalized CHSH Inequalities". In: *Quantum* 5, p. 444. DOI: 10.22331/q-2021-04-26-444 (cit. on pp. 36, 69).

Senellart, P., G. Solomon, and A. White (Nov. 2017). "High-Performance Semiconductor Quantum-Dot Single-Photon Sources". In: *Nature Nanotechnology* 12.11, pp. 1026–1039. DOI: 10.1038/nnano.2017.218 (cit. on p. 37).

Shalm, L. K. et al. (Dec. 2015). "Strong Loophole-Free Test of Local Realism". In: *Physical Review Letters* 115.25, p. 250402. DOI: 10.1103/PhysRevLett.115.250402 (cit. on pp. 11, 15, 16, 111).

Shannon, C. E. (Oct. 1949). "Communication Theory of Secrecy Systems". In: *The Bell System Technical Journal* 28.4, pp. 656–715. DOI: 10.1002/j.1538-7305.1949.tb00928.x (cit. on p. 9).

Simon, C. et al. (May 2010). "Quantum Memories". In: *The European Physical Journal D* 58.1, pp. 1–22. DOI: 10.1140/epjd/e2010-00103-y (cit. on p. 13).

Slussarenko, S. and G. J. Pryde (Dec. 2019). "Photonic Quantum Information Processing: A Concise Review". In: *Applied Physics Reviews* 6.4, p. 041303. DOI: 10.1063/1.5115814 (cit. on p. 3).

Söllner, I., S. Mahmoodian, S. L. Hansen, L. Midolo, A. Javadi, G. Kiršanskė, T. Pregnolato, H. El-Ella, E. H. Lee, J. D. Song, S. Stobbe, and P. Lodahl (Sept. 2015). "Deterministic Photon–Emitter Coupling in Chiral Photonic Circuits". In: *Nature Nanotechnology* 10.9, pp. 775–778. DOI: 10.1038/nnano.2015.159 (cit. on p. 49).

Somaschi, N. et al. (2016). "Near-Optimal Single-Photon Sources in the Solid State". In: *Nature Photonics* 10, 340 EP – (cit. on p. 38).

Stranski, I. N. and L. Krastanow (Dec. 1937). "Zur Theorie der orientierten Ausscheidung von Ionenkristallen aufeinander". In: *Monatshefte für Chemie und verwandte Teile anderer Wissenschaften* 71.1, pp. 351–364. DOI: 10.1007/BF01798103 (cit. on p. 5).

Takeda, S. and A. Furusawa (June 2019). "Toward Large-Scale Fault-Tolerant Universal Photonic Quantum Computing". In: *APL Photonics* 4.6, p. 060902. DOI: 10.1063/1.5100160 (cit. on p. 3).

Tan, E. Y.-Z., P. Sekatski, J.-D. Bancal, R. Schwonnek, R. Renner, N. Sangouard, and C. C.-W. Lim (Dec. 2020). *Improved DIQKD Protocols with Finite-Size Analysis*. DOI: 10.48550/arXiv.2012.08714 (cit. on pp. 81, 82).

Thomas, S. and P. Senellart (2021). "The Race for the Ideal Single-Photon Source Is On". In: *Nature Nanotechnology* 16.4, pp. 367–368 (cit. on p. 37).

Tighineanu, P., C. L. Dreeßen, C. Flindt, P. Lodahl, and A. S. Sørensen (June 2018). "Phonon Decoherence of Quantum Dots in Photonic Structures: Broadening of the Zero-Phonon Line and the Role of Dimensionality". In: *Physical Review Letters* 120.25, p. 257401. DOI: 10.1103/PhysRevLett.120.257401 (cit. on pp. 21, 73, 103).

Tomm, N., A. Javadi, N. O. Antoniadis, D. Najer, M. C. Löbl, A. R. Korsch, R. Schott, S. R. Valentin, A. D. Wieck, A. Ludwig, and R. J. Warburton (2021). "A Bright and Fast Source of Coherent Single Photons". In: *Nature Nanotechnology* 16.4, pp. 399–403. DOI: 10.1038/s41565-020-00831-x (cit. on pp. 5, 16, 22, 30, 32, 34, 35, 69, 77–79, 81).

Trivedi, R., K. Fischer, S. Xu, S. Fan, and J. Vuckovic (Oct. 2018). "Few-Photon Scattering and Emission from Low-Dimensional Quantum Systems". In: *Physical Review B* 98.14, p. 144112. DOI: 10.1103/PhysRevB.98.144112 (cit. on p. 54).

Uppu, R., L. Midolo, X. Zhou, J. Carolan, and P. Lodahl (Dec. 2021a). "Quantum-Dot-Based Deterministic Photon–Emitter Interfaces for Scalable Photonic Quantum Technology". In: *Nature Nanotechnology* 16.12, pp. 1308–1317. DOI: 10.1038/s41565-021-00965-6 (cit. on p. 3).

— (2021b). *Single-Photon Quantum Hardware: Towards Scalable Photonic Quantum Technology with a Quantum Advantage*. arXiv: 2103.01110 [quant-ph] (cit. on p. 21).

Uppu, R., F. T. Pedersen, Y. Wang, C. T. Olesen, C. Papon, X. Zhou, L. Midolo, S. Scholz, A. D. Wieck, A. Ludwig, and P. Lodahl (Dec. 2020). "Scalable Integrated Single-Photon Source". In: *Science Advances* 6.50, eabc8268. DOI: 10.1126/sciadv.abc8268 (cit. on pp. 4, 5, 16, 28, 30, 32, 34, 35, 38, 69, 77, 78, 80, 81, 85).

Ursin, R. et al. (July 2007). "Entanglement-Based Quantum Communication over 144 Km". In: *Nature Physics* 3.7, pp. 481–486. DOI: 10.1038/nphys629 (cit. on p. 7).

Virtanen, P. et al. (2020). "SciPy 1.0: Fundamental Algorithms for Scientific Computing in Python". In: 17, pp. 261–272. DOI: 10.1038/s41592-019-0686-2 (cit. on p. 115).

Walls, D. and G. J. Milburn, eds. (2008). *Quantum Optics*. Berlin, Heidelberg: Springer. DOI: 10.1007/978-3-540-28574-8 (cit. on p. 87).

Wang, H., Z.-C. Duan, Y.-H. Li, S. Chen, J.-P. Li, Y.-M. He, M.-C. Chen, Y. He, X Ding, C.-Z. Peng, et al. (2016). "Near-Transform-Limited Single Photons from an Efficient Solid-State Quantum Emitter". In: *Physical Review Letters* 116.21, p. 213601 (cit. on p. 37).

Wang, H. et al. (2019). "Towards Optimal Single-Photon Sources from Polarized Microcavities". In: *Nature Photonics* 13.11, pp. 770–775. DOI: 10.1038/s41566-019-0494-3 (cit. on pp. 38, 81).

Wang, S. et al. (Feb. 2022). "Twin-Field Quantum Key Distribution over 830-Km Fibre". In: *Nature Photonics* 16.2, pp. 154–161. DOI: 10.1038/s41566-021-00928-2 (cit. on p. 9).

Wang, X., Y. Xiao, C. Liu, E. Lee-Wong, N. J. McLaughlin, H. Wang, M. Wu, H. Wang, E. E. Fullerton, and C. R. Du (Sept. 2020). "Electrical Control of Coherent Spin Rotation of a Single-Spin Qubit". In: *npj Quantum Information* 6.1, pp. 1–6. DOI: 10.1038/s41534-020-00308-8 (cit. on pp. 3, 49).

Wehner, S., D. Elkouss, and R. Hanson (Oct. 2018). "Quantum Internet: A Vision for the Road Ahead". In: *Science* 362.6412, eaam9288. DOI: 10.1126/science.aam9288 (cit. on pp. 1, 7).

Wittek, P. (June 2015). "Algorithm 950: Ncpol2sdpa –Sparse Semidefinite Programming Relaxations for Polynomial Optimization Problems of Noncommuting Variables". In: *ACM Transactions on Mathematical Software* 41.3, 21:1–21:12. DOI: 10.1145/2699464 (cit. on p. 115).

Woodhead, E., A. Acín, and S. Pironio (2020). *Device-Independent Quantum Key Distribution Based on Asymmetric CHSH Inequalities*. arXiv: 2007.16146 [quant-ph] (cit. on p. 36).

— (Apr. 2021). "Device-Independent Quantum Key Distribution with Asymmetric CHSH Inequalities". In: *Quantum* 5, p. 443. DOI: 10.22331/q-2021-04-26-443 (cit. on p. 69).

Wootters, W. K. and W. H. Zurek (1982). "A Single Quantum Cannot Be Cloned". In: *Nature* 299.5886, pp. 802–803. DOI: 10.1038/299802a0 (cit. on pp. 7, 9).

Yin, J. et al. (June 2020). "Entanglement-Based Secure Quantum Cryptography over 1,120 Kilometres". In: *Nature* 582.7813, pp. 501–505. DOI: 10.1038/s41586-020-2401-y (cit. on p. 7).

Yuan, Z., A. Plews, R. Takahashi, K. Doi, W. Tam, A. W. Sharpe, A. R. Dixon, E. Lavelle, J. F. Dynes, A. Murakami, M. Kujiraoka, M. Lucamarini, Y. Tanizawa, H. Sato, and A. J. Shields (Aug. 2018). "10-Mb/s Quantum Key Distribution". In: *Journal of Lightwave Technology* 36.16, pp. 3427–3433. DOI: 10.1109/JLT.2018.2843136 (cit. on p. 9).

Zhai, L., G. N. Nguyen, C. Spinnler, J. Ritzmann, M. C. Löbl, A. D. Wieck, A. Ludwig, A. Javadi, and R. J. Warburton (2021). *Quantum Interference of Identical Photons from Remote Quantum Dots*. arXiv: 2106.03871 [quant-ph] (cit. on p. 23).

Zhang, J., G. Pagano, P. W. Hess, A. Kyprianidis, P. Becker, H. Kaplan, A. V. Gorshkov, Z.-X. Gong, and C. Monroe (Nov. 2017). "Observation of a Many-Body Dynamical Phase Transition with a 53-Qubit Quantum Simulator". In: *Nature* 551.7682, pp. 601–604. DOI: 10.1038/nature24654 (cit. on p. 3).

Zhang, W., T. van Leent, K. Redeker, R. Garthoff, R. Schwonnek, F. Fertig, S. Eppelt, W. Rosenfeld, V. Scarani, C. C.-W. Lim, and H. Weinfurter (July 2022). "A Device-Independent Quantum Key Distribution System for Distant Users". In: *Nature* 607.7920, pp. 687–691. DOI: 10.1038/s41586-022-04891-y (cit. on pp. 13, 68, 69).

Zhang, Y., S. Glancy, and E. Knill (Dec. 2011). "Asymptotically Optimal Data Analysis for Rejecting Local Realism". In: *Physical Review A: Atomic, Molecular, and Optical Physics* 84.6, p. 062118. DOI: 10.1103/PhysRevA.84.062118 (cit. on p. 34).

Zhao, Y. et al. (Apr. 2020). "Frequency-Dependent Squeezed Vacuum Source for Broadband Quantum Noise Reduction in Advanced Gravitational-Wave Detectors". In: *Physical Review Letters* 124.17, p. 171101. DOI: 10.1103/PhysRevLett.124.171101 (cit. on p. 1).

Zhong, H.-S. et al. (Dec. 2018). "12-Photon Entanglement and Scalable Scattershot Boson Sampling with Optimal Entangled-Photon Pairs from Parametric Down-Conversion". In: *Physical Review Letters* 121.25, p. 250505. DOI: 10.1103/PhysRevLett.121.250505 (cit. on pp. 6, 47).

Żukowski, M., A. Zeilinger, M. A. Horne, and A. K. Ekert (Dec. 1993). ""Event-ready-detectors" Bell Experiment via Entanglement Swapping". In: *Physical Review Letters* 71.26, pp. 4287–4290. DOI: 10.1103/PhysRevLett.71.4287 (cit. on p. 6).

Vale.