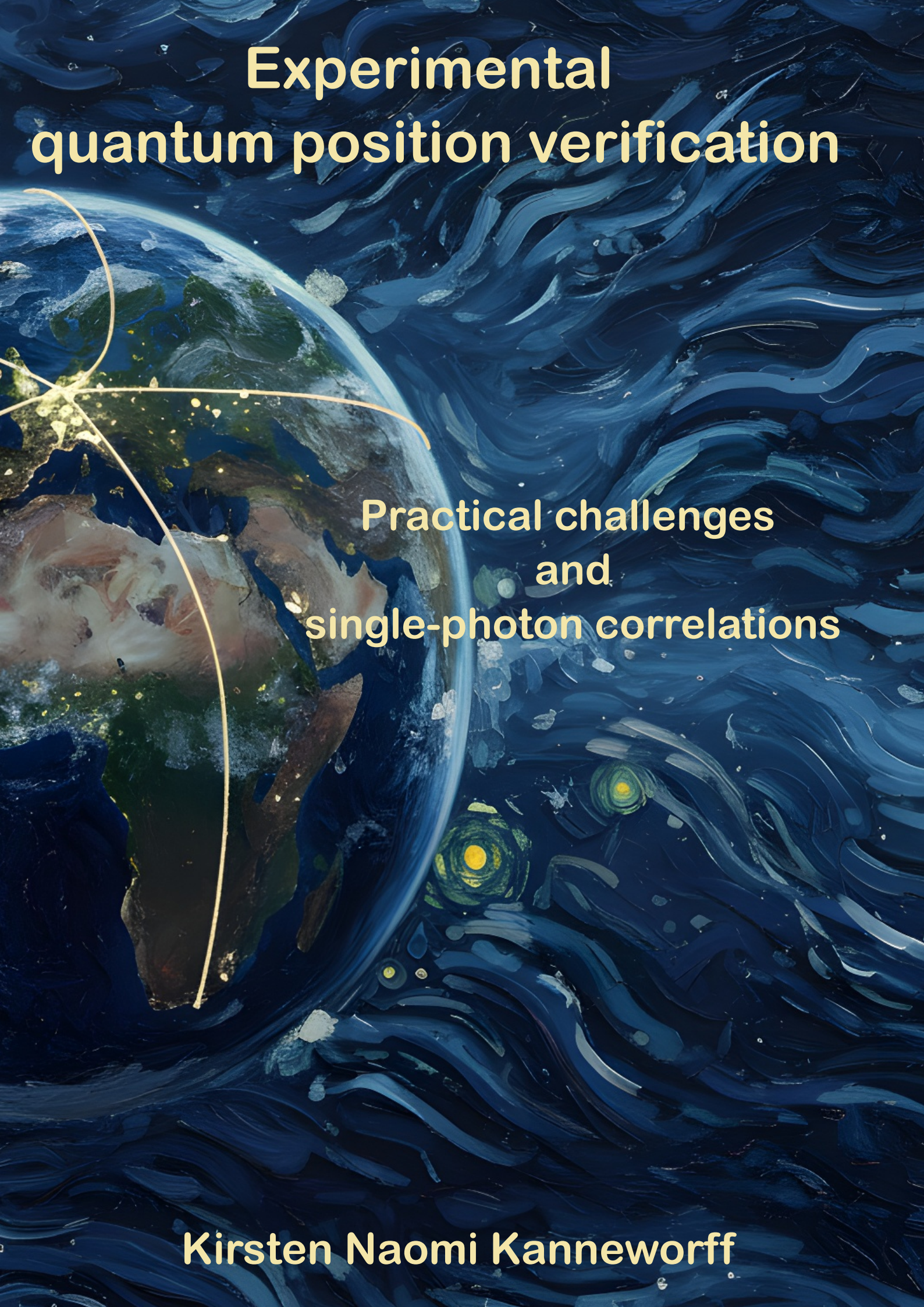
Experimental quantum position verification: practical challenges and single-photon correlations

Kanneworff, K.N.

Experimental quantum position verification



Practical challenges and single-photon correlations

Kirsten Naomi Kanneworff

Experimental quantum position verification: Practical challenges and single-photon correlations

Proefschrift

ter verkrijging van

de graad van doctor aan de Universiteit Leiden,

op gezag van rector magnificus prof.dr. S. de Rijcke,

volgens besluit van het college voor promoties

te verdedigen op woensdag 18 februari 2026

klokke 14:30 uur

door

Kirsten Naomi Kanneworff

geboren te Zwijndrecht, Nederland

in 1996

Promotores: Dr. W. Löffler

Prof.dr. D. Bouwmeester

Promotiecommissie: Prof.dr. H.M. Buhrman (Universiteit van Amsterdam, Netherlands)

Prof.dr. E. Diamanti (Université Paris-Sud, France)

Prof.dr. M.P. van Exter

Prof.dr.ir. S.J. van der Molen

Dr. E.P.L. van Nieuwenburg

Prof.dr.ir. T.H. Oosterkamp

An electronic version of this thesis can be found at https://scholarlypublications.universiteitleiden.nl/

The research project described in this thesis was conducted at the Leiden Institute of Physics, Leiden University. The project received funding from the Netherlands Organization for Scientific Research (NWO/OCW) through the Quantum Software Consortium (project number 024.003.037 / 3368), from the Dutch Ministry of Economic Affairs through Quantum Delta NL (project number NGF.1582.22.025) and from the European Union's Horizon 2020 research and innovation program under grant agreement No. 862035 (QLUSTER).

Printing: Ridderprint|www.ridderprint.nl

The cover image is an AI-generated impression of quantum position verification around the Earth, inspired by the painting De Sterrennacht by the Dutch painter Vincent van Gogh.

Natuurkunde is het mooiste vak dat er is.

J. Bruijstens (docent natuurkunde)

Contents

1 Introduction

Everyone has dealt with fraudulent emails where a criminal sender pretends to be with your bank and tries to trick you into entering personal information on another website. Checking if someone is who they claim to be is known as authentication. Authentication methods generally fall into three categories: knowledge, ownership, and inherence. These are collectively known as authentication factors. Knowledge refers to something a person knows, such as the personal identification number (PIN) code of a bank card or the password to an email account. Ownership involves authentication through something a person possesses, for example, an ID card. Inherence relates to something inherent to the individual. Well-known examples include fingerprint and facial profiles, which are nowadays often used to unlock phones or other devices.

Most forms of authentication require individuals to meet in person. For example, how else can one verify that an ID card belongs to the person presenting it? However, with people and systems increasingly connected across the globe via the internet, requiring physical presence for authentication is often impractical and burdensome. Could the geographical location of a person or a computer serve as a means of authentication without the need for in-person verification? The estate of important enterprises, including banks and computing centers, is usually very well protected, and therefore, confirmation that a party or computer is indeed located at a certain position would be a pretty strong indication that one is communicating with the desired party! The use of the geographical location for authentication is the basis of position verification.

1.1 Position verification

Position verification requires multiple parties, similar to global positioning systems, where one requires multiple satellites to determine a position; the reversed process of position verification requires at least two trusted parties to confirm the position of a third party. We imagine the following scenario: for online banking, one wishes to ensure that communication occurs with a computer at the geographic location of the bank. This location is known, and therefore, so is the distance between the two trusted parties and the bank. We simplify the situation by reducing our three-dimensional world into a single dimension – a straight line – but the principle can be extended to more dimensions. This one-dimensional world is depicted in Fig. 1.1, where one party (e.g., you) is separated by a distance d to the left side of the bank. On the opposite side, you have a trusted friend at the same distance. In position verification, the party whose position should be certified is called the prover because they have to prove their location to you. The trusted parties are known as the verifiers because they wish to verify the position of the yet untrusted party.

The distance between the verifier and the prover can be determined by the verifiers, who transmit signals to the prover and record the timing of the answers of the provers. Position verification relies on the fundamental speed limit at which any physical information can

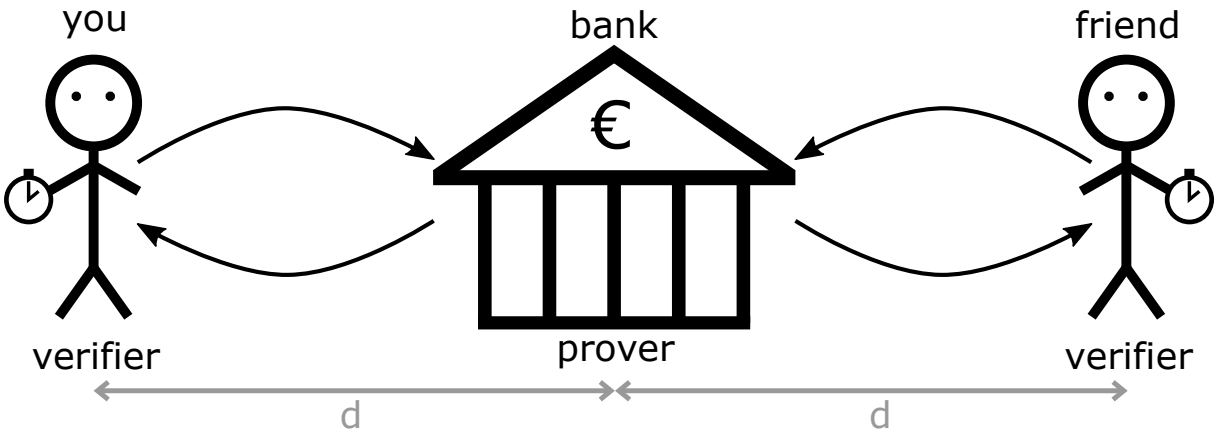


Figure 1.1: Cartoon of position verification where you and your friend (verifiers) wish to verify the position of a third person in e.g. a bank (prover) by confirming the distance d, by sending signals and timing the responses.

propagate, the speed of light given by the theory of special relativity. Information encoded into light and other electromagnetic waves travels through the atmosphere at nearly the speed of light, making electromagnetic waves ideal for distance measurement. To optimize distance determination, it is beneficial for the verifiers to ensure that information from both sides reaches the prover simultaneously. Usually, the prover is given a computational task that they have to perform with the information received from both verifiers, such as a bitwise XOR operation. The prover returns the result to the two verifiers, who then check both the outcome and the timing to determine whether the prover is indeed at the claimed position. These checks require communication between the verifiers, whose communication channel is assumed to be both private and secure.

1.2 Classical position verification

In order to explore if the position of the prover can be securely certified using only classical information, we have to consider the worst-case attack scenario. In this scenario, two or more adversaries intercept all communication with the prover and communicate with the two verifiers as shown in Fig. 1.2. The goal of these thieves is to convince the verifiers that they are located at the position of the bank, even though they are never allowed to be inside the premises of the bank. At least two adversaries are required in the scenario shown in Fig. 1.2, where we assume that the adversaries are in full control of all communications. All the information sent by the verifiers needs to be used in order to successfully replicate the task set for the prover. If there were only one adversary, it would take too long to respond to either verifier since the adversary is further away from one verifier than the bank would have been. Therefore, as a rule, at least one adversary per verifier is required to perform a useful attack.

In the worst-case attack scenario, the adversaries intercept all communication from the verifiers. Each adversary produces a perfect copy of the received information (as illustrated in Fig. 1.2) and transmits this copy to the other adversary. As a result, both adversaries possess all the information required to perform the same operation as the prover. Consequently, they are able to return the correct answers to the verifiers. Since the total distance that the information travels is the same as in the case without

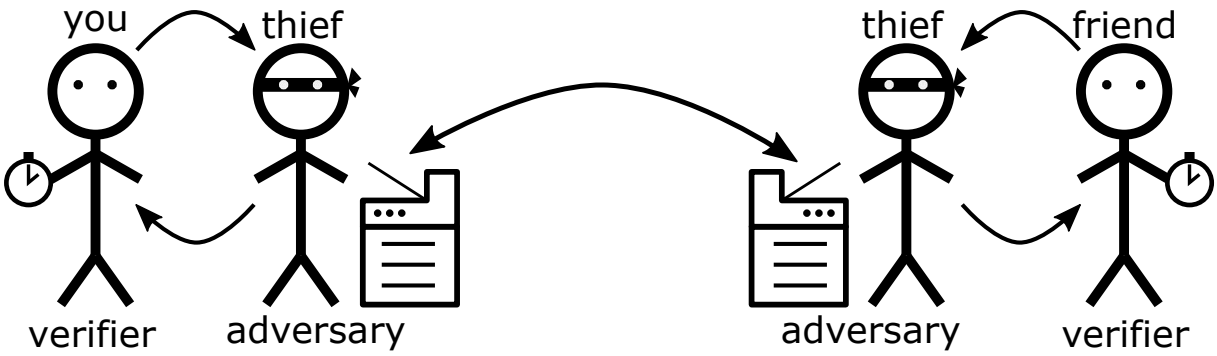


Figure 1.2: Cartoon of position verification where instead of the bank (prover) there are two thieves (adversaries) pretending to be in the bank. Both thieves have a copy machine at their disposal with which they can copy the information intercepted from the verifiers.

adversaries, and no repeated communication between the adversaries is required, the adversaries are able to respond within the expected time. This renders classical position verification inherently insecure.

We note that we are here exclusively discussing position verification in which the prover and the verifiers do not share a private key. If a shared key were available, the prover could perform a cryptographic operation that makes position verification simple. However, this approach would require the verifiers and prover to meet in person, which, as noted before, is impractical on a global scale.

1.3 Quantum position verification

Luckily, the attack described above is only possible when only classical information is used. Quantum information cannot be copied perfectly, which is stated by the no-cloning theorem. This means adversaries cannot simply duplicate the quantum information from the verifiers, and the attack described before is not possible. This is the foundation of quantum position verification (QPV): In each round of the protocol, at least one of the exchanged signals must be quantum [1]. In QPV, quantum information in the form of qubits is encoded into a degree of freedom of photons, such as the photon frequency, timing, or polarization. In this thesis, we will focus on single photons where the qubit is encoded in the photon polarization.

QPV was first presented in a patent in 2006 [2] and further investigated in the 2010s [3–16]. From 2020 onward, interest and research into this topic increased strongly [17–35]. Over the past two decades, various QPV protocols have been proposed, all following the fundamental principles outlined before. The main differences between these protocols lie in the combination of classical and quantum information that is transmitted and received, as well as in the specific tasks assigned to the prover. In the first protocols, only one verifier sends quantum information, but for these protocols it was found that total loss must be below 50%. This limitation is significant, as photon loss is large also in free-space transmission. With this in mind, protocols that are fully loss tolerant were proposed and investigated. These protocols involve sending two qubits, one by each verifier, and are based on quantum interference effects. One of these protocols is the SWAP protocol by Allerstorfer et al. [17] which will be at the core of this thesis.

1.4 Scope of the thesis

In this thesis, we show our work towards an experimental demonstration of the SWAP QPV protocol using a temporally demultiplexed quantum dot single-photon source. In Chapter 2, we provide an in-depth overview of the field of quantum position verification by describing different well-known protocols and adversarial attacks under specific conditions. Furthermore, we outline the main considerations for QPV implementations, including loss tolerance, resilience against adversaries with pre-shared entanglement, and the potential use of fiber-based networks for transmitting quantum information. We also provide a mathematical description of the radius of a trusted region that needs to be installed to avoid attack strategies caused by either slow information exchange or non-instantaneous prover operations.

In Chapter 3, we investigate the encoding of polarization qubits with fiber-based polarization modulators and the transport of photons over long optical fibers, and assess the stability of these devices for use in a QPV experiment.

In Chapter 4, we investigate the single-photon indistinguishability of our quantum dot single-photon source for different temporal delays in a Mach-Zehnder interferometer (MZI). We derive an analytical framework to describe not only the zero-time correlations, but also correlations for a time equal to the temporal delay in the interferometer. Furthermore, we develop a model for single-photon indistinguishability that includes many experimental imperfections.

In Chapter 5, we study quantum interference and photon correlations in an experiment where a single-photon stream is deterministically temporally demultiplexed using a fast fiber switch, and synchronized and interfered at a beam splitter. We develop a model that describes photon correlations when the photon rate exceeds the switching rate, and we compare the model with experimental data, highlighting the importance of correct normalization of the experimental coincidence events.

In the final chapter, we show a first experimental demonstration of quantum position verification in a laboratory environment. By comparison of our experimental data to a theoretical model, we identify the most important experimental factors relevant for future QPV implementations. Our QPV experiment does not yet demonstrate fully-secure QPV, since the protocol is not resilient against attackers with pre-shared entanglement and due to imperfections of our single-photon source. We show how those issues can be mitigated in the future.

2 Quantum position verification

The goal of the research presented in this thesis is to work towards a demonstration of quantum position verification (QPV) in a laboratory environment using single photons. In this Chapter, we give an overview of selected proposed QPV protocols and discuss attack strategies. This relates to unavoidable challenges that arise in both future QPV implementations and current experiments, such as photon loss, noise, delays in prover operations, and slow quantum information transfer. We also discuss the resilience of QPV protocols against adversaries with access to pre-shared entanglement. We introduce the concept of a trusted region around the prover and discuss how this can partially mitigate issues. Finally, we give an overview of several QPV protocols and compare them with respect to the aforementioned issues.

2.1 Early protocols

2.1.1 BB84 QPV protocol

The QPV_{BB84} protocol, also known as the measurement protocol, is one of the earliest proposed QPV schemes [4]. It is based on the well-known quantum key distribution (QKD) BB84 protocol, introduced by Bennett and Brassard in 1984 [36]. Although QPV_{BB84} builds on a QKD protocol, its objective is different. In QPV, the goal is to authenticate a node in order to expand an existing network, whereas in QKD, the goal is to share private keys between nodes that have already been authenticated. An easy way to represent the information send by the verifiers (V_0 and V_1) and returned by the prover (P) is through a space-time diagram. The space-time diagram depicting the QPV_{BB84} protocol is shown in Fig. 2.1, where the prover P is positioned exactly in the middle between verifiers V_0 and V_1. The curly lines in the space-time diagram denote quantum information, and straight lines denote classical information.

In the measurement protocol, one verifier (V_1 in this example) sends a qubit state, while the other verifier (V_0) sends, as classical information, the basis in which the state should be measured by P. Throughout this thesis, all discussions of QPV protocols will be related to implementations based on single photons, as these are the primary focus of our research. The prover sends the measurement outcome in the form of classical information back to both verifiers. This process is done multiple times, also known as rounds. In the end, the verifiers check if the responses they get from P are correct and have arrived at the expected time. This time is given by $t = 2d/c$ where d is the distance between the verifiers and the prover (Fig. 2.1), and c is the speed of light. The verifiers also check if each got the same response for every round and if all results together follow the expected distribution of answers. In the case of the QPV_{BB84} protocol the prover should always return the correct outcome.

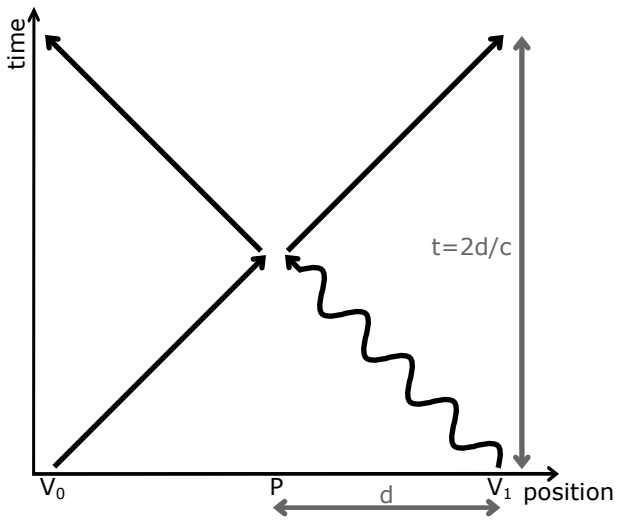


Figure 2.1: Space-time diagram of the QPV_{BB84} protocol. The curly arrow symbolizes quantum information and the straight arrows classical information.

2.1.2 The routing QPV protocol

The routing protocol was proposed at the same time as the measurement protocol and is quite similar to the QPV_{BB84} protocol [4]. However, in the routing protocol, the prover task is to use the classical information sent by V_0 to determine whether the qubit (e.g. single photon) should be forwarded to V_0 or should be returned to V_1. P also sends the classical information received by V_0 to both verifiers for the timing check. The verifier who receives the quantum state measures the state to determine whether the quantum information is genuine. As in QPV_{BB84}, this process is repeated over multiple rounds. Finally, the verifiers again check the timing and the distribution of the outcomes required to certify the position of the prover.

2.1.3 BB84 QPV protocol attacks

We now consider the scenario in which two adversaries are positioned around the prover location, and who try to convince the verifiers that they are at the location of P, even if they are not – the adversaries are not permitted to be at the location of the prover. The task assigned to the prover is publicly known, but all information sent by the verifiers in a single round is required to perform the task successfully. Therefore, assuming for now that the adversaries do not possess pre-shared entanglement, no attack strategy allows them to always return the correct response and remain within the expected timing, as illustrated in Fig. 2.2(a).

Another attack strategy of the adversaries is to guess the measurement result to respond within the time constraint $t = 2d/c$. One such attack is depicted in Fig. 2.2(b), where adversary A_1 chooses a random basis to measure the qubit sent by V_1. Assuming that the verifiers use only two of the 3 bases following BB84 [36], A_1 has a 50% chance to guess the basis correctly, and the measurement outcome will be correct. If A_1 has chosen the wrong basis, there is still a 50% chance the outcome of the measurement is guessed correctly. In total, the adversaries will guess the answer of the prover correctly with a chance of 75%, which can easily be detected since the prover at the correct position will always return the correct answer. In summary, the adversaries either fail to meet the timing constraints, or they must guess the answer and consequently do not satisfy the expected answer statistics.

Up to now, we have assumed ideal conditions, in particular that every photon qubit sent by V_1 is detected and responded to by the prover. In reality, optical transmission, either through free-space or through fiber-based optical networks, is subject to loss. As a result, there will be rounds in the QPV protocol where the prover does not report an answer and declares loss. This loss opens up a new attack strategy for the adversaries depicted in Fig. 2.2(b) by the blue dotted lines. Here, A_0 copies the classical information containing the basis information and sends one copy to A_1 ($\cdot-$ line) and keeps the other copy for themselves ($\cdot\cdot$ line). A_1 chooses a random basis and sends this basis and the measurement result to A_0. Once both adversaries have the information on the actual basis, they check if the basis choice made by A_1 was correct. If so, they return the answer to the verifiers, and if not, they declare that the photon was lost. It has been shown that these early types of QPV protocols, where the information is encoded in one of two bases, are only secure against such types of attacks if the transmission probability of the communication channel exceeds 3dB (50%) [8]. We call this a partially loss-tolerant protocol.

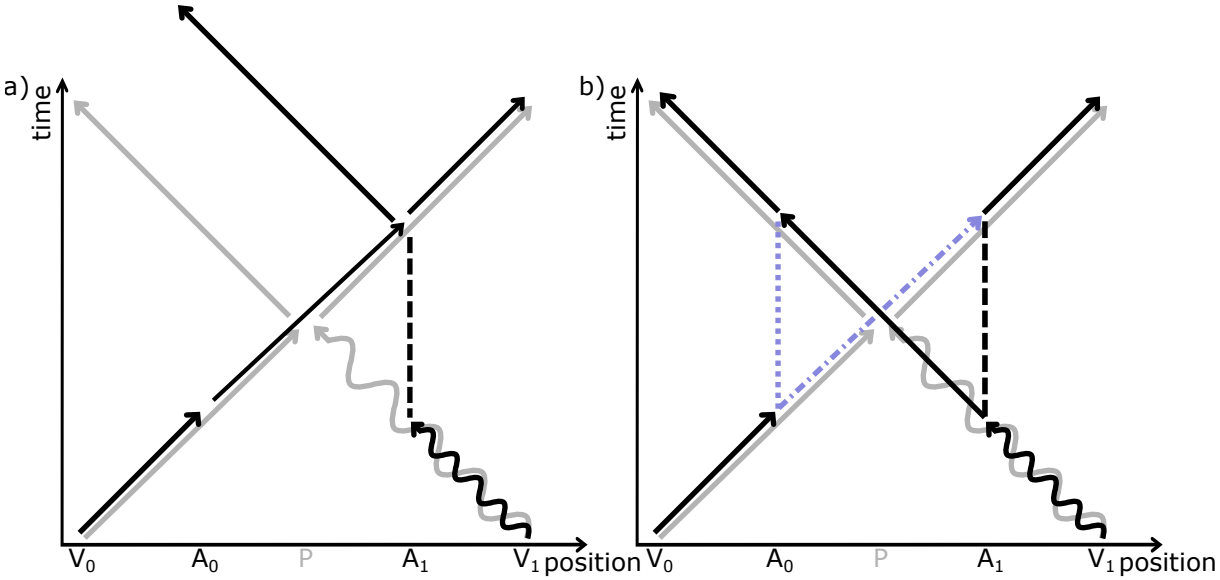


Figure 2.2: Space-time diagrams depicting possible attacks by adversaries A_0 and A_1, where A_1 performs the same task as set for the prover (a), or A_1 guesses the outcome (b). The space-time diagram corresponding to the QPV_{BB84} protocol for the prover P from Fig. 2.1 is shown in gray as reference. The blue ($\cdot-$ and $\cdot\cdot$) lines in (b) depict a guessing attack under the condition of single photon/qubit loss.

2.2 Two-photon protocols

A QPV protocol that is not susceptible to this loss-based attack we call fully loss-tolerant, one such protocol we discuss now. Each verifier sends one photon qubit, and the task of the prover is to decide if the qubits were equal or not. Within certain probability limits, this is a task doable in quantum optics, using the Hong-Ou-Mandel effect [37].

2.2.1 The Lim QPV protocol

The first proposal of such a two-photon QPV protocol was published by Lim et al. [12], where each verifier sends one qubit in the form of a polarization encoded single photon. For each round, the verifiers agree on the same basis (two options), and each randomly chooses one of its two states. The prover task is to determine whether the two polarization states were the same ($\|$) or orthogonal ($\perp$) to each other. This determination can be done by performing a (partial) Bell-state measurement (BSM). The outcome of the task is returned in the form of classical information (Fig. 2.3).

The Bell-state measurement is based on Hong-Ou-Mandel (HOM) quantum interference where fully indistinguishable photons, i.e. photons with the same polarization state ($\|$), always exit a 50:50 beam splitter through the same output port (Fig. 2.4(a)) [37, 38]. If the photons are fully distinguishable ($\perp$), the photons are independently distributed by the beam splitter, exiting with 50% chance the beam splitter through the same port. Therefore, if the photons exit through different output ports, the prover knows that the polarization states were orthogonal, if they exit through the same port this can be due to the HOM effect or just by chance.

Most single-photon detectors cannot determine the exact number of photons in a single

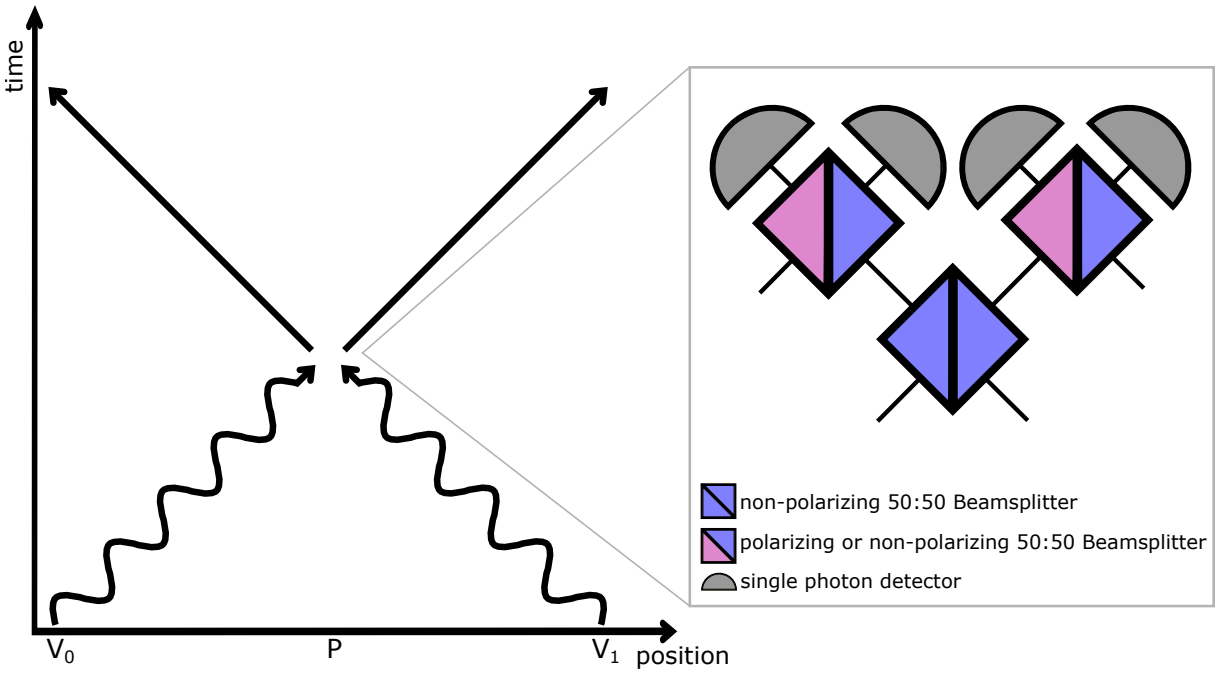


Figure 2.3: Space-time diagram of a two-photon QPV protocol, the inset shows a schematic of the prover task: a partial Bell-state measurement (BSM), where the bottom beam splitter is non-polarizing whilst the two top ones are either polarizing beam splitters following the Lim protocol or non-polarizing beam splitter following the SWAP protocol [17].

pulse. As a result, they cannot distinguish between the case where two photons exit through the same port (Fig. 2.4(a)) and the case where only one photon is detected because the other was lost before reaching the beam splitter (Fig. 2.4(b)). To address this limitation, Lim et al. introduced additional polarizing beam splitters (Fig. 2.3). This setup ensures that the prover can give a conclusive answer—whether the incoming states were parallel or orthogonal—only when two detection events occur simultaneously. The combination of post-selection on two detector events and the fact that the polarization basis used to encode the photons remains private between the verifiers results in this type of QPV protocol being fully loss tolerant.

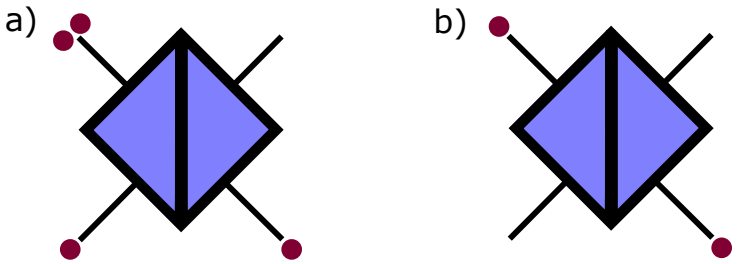


Figure 2.4: Photon bunching versus loss: without photon-number resolving detectors we cannot discriminate between the case where two photons exit through the same output port (a) and the case where only one photon arrived because the other was lost (b).

2.2.2 Lim QPV protocol attacks

Lim et al. investigated an attack strategy with adversaries that are limited to local operations and classical communication (LOCC), i.e., they can modify or measure quantum states at their own location and communicate only with classical signals. The attack strategy discussed by Lim et al. is similar to the one explained previously for the $\mathrm{QPV}_{\mathrm{BB84}}$ protocol based on guessing: Adversaries A_0 and A_1 choose a random basis which they communicated before, and both measure their own photon in this basis. They share their classical outcomes from which they determine whether or not the polarization states were the same, and return this answer to the verifiers. If the adversaries have chosen the correct basis, which happens with probability 1/2, their answer is correct. If the adversaries had chosen the wrong basis, there is still a possibility that they obtain the correct answer with probability 1/2. Therefore, like with the $\mathrm{QPV}_{\mathrm{BB84}}$, the total guessing probability is 3/4 - now, however, the protocol is fully loss tolerant [12].

2.2.3 The SWAP QPV protocol

The protocol proposed by Allerstorfer et al. [17] is a modified version of the Lim protocol, in which the polarizing beam splitters are replaced with non-polarizing 50:50 beam splitters, see Fig. 2.3. This modification offers two advantages: First, the setup does not include any polarization-sensitive elements, therefore, the absolute choice of the polarization basis is irrelevant. The experiment only tests whether the qubit states are equal or orthogonal. This simplifies the use of fiber-based networks, as optical fibers modify the polarization of the transmitted light. Secondly, whereas in the proposal of Lim et al. the verifiers had two basis choices to their disposal, now all three polarization bases can be used. The additional basis reduces the probability that adversaries are guessing the correct basis. This guessing probability of the adversaries under the LOCC condition reduces from 3/4 to 2/3 [17].

It was later proven by Allerstorfer et al. [18] that the SWAP protocol is also resilient against more sophisticated attacks where the adversaries are able to use quantum communication (LOQC).

2.2.4 Attacks using pre-shared entanglement

It has been shown that two-photon QPV protocols are fully loss tolerant and are resilient against attacks under LOCC and LOQC conditions. However, it has also been shown that any proposed QPV protocol can be broken by adversaries if they possess sufficient amounts of pre-shared entanglement [15]. The exact meaning of 'sufficient' depends on the details of the specific protocol. For the protocols discussed in previous section, an attack can be successful if the adversaries have a single entangled pair of qubits per round (linear scaling). We note that in order to be successful, the adversaries must be able to perform a perfect quantum teleportation operation, which is extremely challenging. Anyway, in later developments, both the $\mathrm{QPV}_{\mathrm{BB84}}$ and the routing protocol have been extended with improved cryptographic tasks for the prover involving increased amounts of classical information from both verifiers. These are known as the *functional* QPV protocols, and have been proven to be secure against adversaries with a linear amount of pre-shared entanglement [23, 28]. Since it is very easy to increase the amount of classical

information, but it is very hard to increase the amount of pre-shared remote entanglement, these protocols can be considered to be secure.

2.3 Experimental considerations

2.3.1 Prover processing time and safety radius

Up to now, we have assumed that the prover task is completed instantaneously. In practice, however, performing any task requires a nonzero amount of time and there is a prover processing time or latency t_m between the time when the prover have received the photons from the verifiers and the time when they return the answer to the verifiers. This delay introduces an uncertainty in determining the position of the prover, and enables an attack strategy if the adversaries have a shorter processing time. In Fig. 2.2(a), we showed that, if the adversaries attempt to perform the prover task perfectly, one of their responses will inevitably be returned too late. Due to the additional time t_m, if the adversaries A_0 and A_1 are close enough to P and have a shorter processing time, they are able to perform the prover task within the time limit. An example of such an attack on a two-photon QPV protocol is shown in Fig. 2.5(a). Here, similar to the attack depicted in Fig. 2.2(a), A_0 forwards their qubit to A_1 who performs the Bell-state measurement (Fig. 2.3). A_1 returns the answer to both sides such that both verifiers receive the answer in the expected time which we indicate by Δt_0.

In order to prevent this type of attack, we must design a trusted region that is inaccessible to adversaries around the position of the prover. The radius r of this trusted region is determined by comparing the total time required for a single QPV round in the honest-prover case, Δt_0, to the total time required by the adversaries, Δt_A. We now introduce distances relative to the prover, d, a_0, and a_1 are the distances between the prover and V_0, A_0, and A_1, respectively. We use v_q and v_c for the velocities of the quantum and classical signals sent by the verifiers, and v_a for the velocity of communications between the adversaries. We assume that adversary A_1 performs the prover task. From the space-time diagram in Fig. 2.5(a) we obtain

$$\begin{aligned} \Delta t_0 =& \frac{d}{v_q} + t_m + \frac{d}{v_c} \\ \Delta t_A =& \frac{d - a_0}{v_q} + 2\frac{a_0 + a_1}{v_a} + \frac{d - a_0}{v_c}. \end{aligned} \tag{2.1}$$

We want to find the minimum required distance of adversary A_1 from the prover, a_1, which is equal to radius of the trusted region r, $r = a_1$. By solving $\Delta t_A = \Delta t_0$ for r we find

$$r = a_1 = \frac{v_a}{2} t_m + \left(\frac{v_a}{2v_q} + \frac{v_a}{2v_c} - 1 \right) a_0. \tag{2.2}$$

The case that A_0 performs the prover task is analogous. For the case that all information travels at the speed of light c, Eq. 2.2 reduces to

$$r = \frac{1}{2} c t_m, \tag{2.3}$$

showing that, in this case, the radius of the necessary trusted region r only depends on t_m.

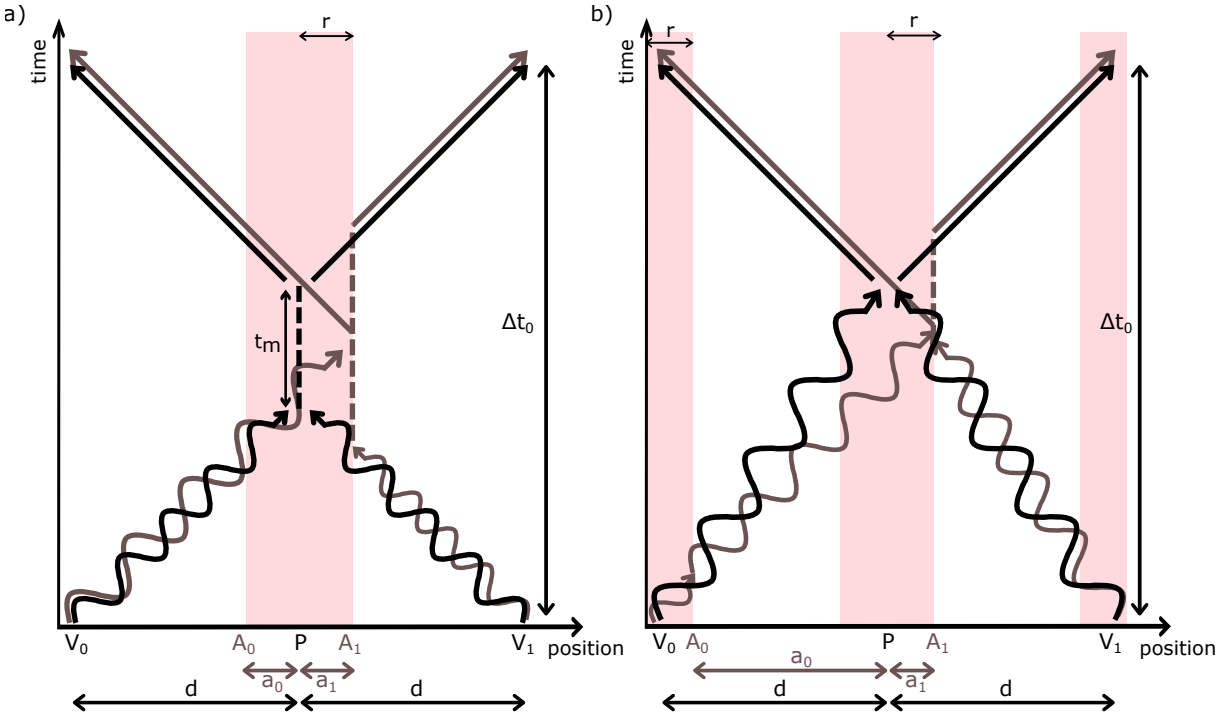


Figure 2.5: Space-time diagram of the two-photon QPV protocol with a non-zero processing or measurement time t_m of the prover (a) or slow quantum communication (b). For each case, the attack strategy explained in the text is shown in gray. The necessary trusted region around the prover and verifiers is shown by the red-shared area.

2.3.2 Slow quantum information transport

A related attack strategy arises if information is sent slower than the speed of light. For example, transmitting photons through an optical fiber network rather than through free space reduces the signal velocity to approximately $2/3c$. The reduced velocity enables attacks if the adversaries can send signals faster, as shown in Fig. 2.5(b). The attackers now must be positioned asymmetrically around the prover. Both A_0 and A_1 intercept the qubit from their respective verifier, A_1 stores their qubit and A_0 uses their faster channel to forward the intercepted qubit to A_1. This qubit can arrive earlier at A_1 as it would have arrived at P due to the slower channels used by the verifiers, A_1 performs the prover task and returns the answer to both verifiers. This can happen within the honest-prover time constraint, and we can again calculate the maximum radius of the trusted region r from Eq. 2.2 by setting $t_m = 0$, and we obtain

$$r = a_1 = \left(\frac{v_a}{2v_q} + \frac{v_a}{2v_c} - 1 \right) a_0. \tag{2.4}$$

As an example, if the quantum information is sent through conventional fibers with $v_q = 2/3c$, the classical information is sent e.g. via radio transmitters with $v_c = c$, and if we assume that the adversaries have access to better resources and can transmit quantum information at the speed of light $v_a = c$, we obtain

$$r = a_1 = \frac{1}{4} a_0. \tag{2.5}$$

This shows that, the radius of the trusted region is only dependent on the distance between A_0 and P, a_0, and the velocity difference.

We now set the trusted region around the prover and both verifiers to be the same size, such that the minimum distance between A_1 and P is $a_1 = r$ and the maximum distance between A_0 and P is $a_0 = d - r$. Using the same assumptions on the signal velocities as before, we obtain a minimum trusted radius around both verifiers and the prover of $r = \frac{1}{5}d$: The trusted region must be at least one fifth of the distance between verifier V_0 and the prover. This poses a serious limitation on QPV using standard optical fibers. Two solutions are investigated currently: First, the use of modern micro-structured hollow-core fibers where the group velocity approaches the speed of light in vacuum [39–41]. Secondly, by combination of classical information traveling at the speed of light with a commitment step [19]: In this approach, the prover first receives the quantum information, stores it, and announces its reception. Only then the prover receives the classical information which is transmitted at the speed of light and that is necessary to perform the prover task. Another advantage of such commitment protocols is, that, the travel time of quantum information becomes completely irrelevant. This is important in optical fiber networks where fibers usually do not follow the shortest path. A disadvantage is, that, storing quantum information with high efficiencies and fidelities is non-trivial.

In conclusion, any source of time delay, whether it arises from the prover processing time or from slow signal velocities, introduces an uncertainty in the positioning of P and requires definition for trusted regions around the prover and the verifiers. The general formula for the radius of this trusted region is:

$$r = \frac{v_a v_c \left(v_q t_m + d\right) + v_a v_q d - 2 v_c v_q d}{v_a \left(v_c + v_q\right)} \tag{2.6}$$

2.4 Conclusions and QPV protocol overview

	$\mathrm{QPV}_{\mathrm{BB84}}$ routing	Two-photon	$\mathrm{QPV}^{f}_{\mathrm{BB84}}$	c-$\mathrm{QPV}^{f}_{\mathrm{BB84}}$
Loss tolerance	partial (3dB[1]) [8]	full [12]	partial (3dB[1]) [23]	only transmission loss [19]
Slow quantum	no [28]	no	yes [29]	yes [19]
Pre-shared entanglement	linear [29]	linear	> linear [28]	> linear [19]

Table 2.1: Overview of the security constraints of several QPV protocols: the BB84 $\mathrm{QPV}_{\mathrm{BB84}}$ and routing protocols [4, 5], two-photon protocols [12, 17], the functional protocol $\mathrm{QPV}^{f}_{\mathrm{BB84}}$ [23], and the commitment and functional protocol $c - \mathrm{QPV}^{f}_{\mathrm{BB84}}$ [19].

[1]This is the worst case loss tolerance where the qubit is encoded in one of two bases. It has been shown that additions of bases can increase the loss tolerance up to 13dB for $\mathrm{QPV}_{\mathrm{BB84}}$ [8, 11] and 70% for $\mathrm{QPV}^{f}_{\mathrm{BB84}}$ [26, 28]

In this Chapter, we have discussed various quantum position verification protocols and the types of attacks adversaries can carry out due to realistic imperfections, such as the loss of quantum signals or signal velocities less than the speed of light in fiber-based networks. Additionally, we mentioned the impossibility of secure QPV against adversaries with a sufficient amount of pre-shared entanglement. The holy grail in QPV research is to design and implement a protocol that exhibits full loss tolerance, allows for slow quantum information transfer, and remains secure even if adversaries have access to large amounts of pre-shared entanglement. As shown in the overview in Table 2.1, steps are made into this direction.

3 Polarization in long fibers and modulators

As discussed in the previous chapter, many quantum position verification (QPV) schemes, and particular those which we discuss in this thesis, rely on manipulation and transmission of polarization-encoded photonic qubits. In order to achieve a lab-based experimental demonstration of such a QPV scheme, one needs to be able to simulate long distances, which is most practical using optical fibers. However, polarization states often change when propagating through fiber-based optical components by stress and strain, which can be used for polarization modulation but also appears due to uncontrolled environmental effects. The environmental effects can be mitigated if the polarization state changes unitarily. In this chapter, we investigate the operation and polarization stability of fiber-based polarization modulators used to prepare polarization qubits, and the transport of such qubits through 200 m-long single-mode fibers that will be used for qubit transport between the QPV nodes. First, a general background about polarization optics is discussed, after which we delve into the question of whether or not the action by the fiber-optic elements can be described as unitary transformations. Next, we examine the stability of a fiber-based polarization modulator, followed by an investigation of the long-term polarization stability of a single-mode fiber. The chapter concludes with a discussion and estimation of polarization mode dispersion in an optical fiber.

3.1 General polarization optics

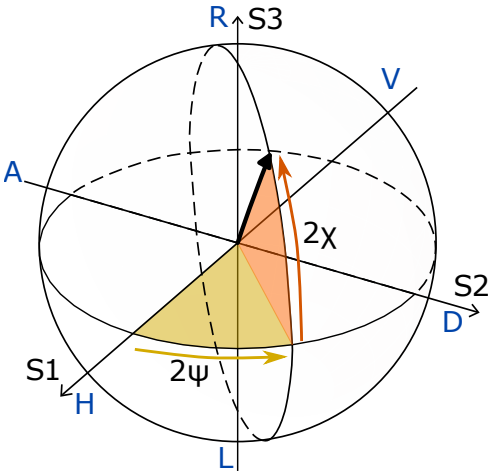


Figure 3.1: Depiction of the Poincaré sphere.

The polarization of light describes the geometrical orientation of the oscillations of, for instance, the electric field vector of light [42]. In a plane transverse to the optical axis, polarization can be described in 3 orthonormal and mutually unbiased bases: the horizontal (H) - vertical (V) basis, the diagonal (D) - anti-diagonal (A) basis, and the right (R) and left (L) circular basis. In the first two linear bases, the field vector oscillates in a plane, while in the circular basis, the field rotates around the optical axis.

The polarization space is visualized by the Poincaré sphere, which is mathematically equivalent to the qubit Bloch sphere, depicted in Fig. 3.1. There, the H/V, D/A, R/L polarization states lie on the x,y, and z axes of the sphere, respectively. Polarization states can also be described by using the Stokes parameters $S_{0...3}$, where S_0 describes the intensity and the Stokes parameters S_1, S_2 and S_3 give the distribution of the intensity in the {H,V}, {D,A}, and {R,L} bases, respectively:

$$\begin{aligned} S_0 &= I_\mathrm{H} + I_\mathrm{V} \\ S_1 &= I_\mathrm{H} - I_\mathrm{V} \\ S_2 &= I_\mathrm{D} - I_\mathrm{A} \\ S_3 &= I_\mathrm{R} - I_\mathrm{L} \end{aligned} \tag{3.1}$$

The Stokes formalism is very useful to describe realistic states of polarization, including not fully polarized (depolarized) light. The Stokes parameters can be related to the spherical coordinate angles (see Fig. 3.1) by using the normalized Stokes parameters s_1, s_2 and s_3, where $s_i = S_i/S_0$:

$$\begin{aligned} s_1 &= p\cos(2\chi)\cos(2\psi) \\ s_2 &= p\cos(2\chi)\sin(2\psi) \\ s_3 &= p\sin(2\chi) \end{aligned} \tag{3.2}$$

The angles ψ and χ are the polarization azimuth and ellipticity, respectively, and p denotes the degree of polarization (DOP). We add the zeroth normalized Stokes parameter $s_0 = 1$. We can then express the polarization density matrix with the normalized Stokes parameters using the Pauli matrices σ_1, σ_2, and σ_3, and as the zeroth Pauli matrix the identity matrix $\sigma_0 = I$:

$$\rho = \frac{1}{2}\left(s_0\sigma_0 + s_1\sigma_1 + s_2\sigma_2 + s_3\sigma_3\right) = \frac{1}{2}\begin{pmatrix} s_0 + s_1 & s_2 - is_3 \\ s_2 + is_3 & s_0 - s_1 \end{pmatrix} \tag{3.3}$$

Fidelity of polarization states

In this chapter, we want to investigate various polarization effects in a way that is directly relevant for a future QPV experiment. Therefore, we evaluate the polarization behavior

of optical components not in terms of the Stokes parameters but in terms of fidelities between different polarization states - this provides direct information on the usability of the components for QPV. The fidelity between two quantum states defined by density matrices ρ_1 and ρ_2 is defined by [43]

$$F(\rho_1, \rho_2) = \left(\mathrm{Tr} \sqrt{\sqrt{\rho_1} \rho_2 \sqrt{\rho_1}} \right)^2 . \tag{3.4}$$

The square roots are well defined since ρ_1 and ρ_2 are both Hermitian, as seen in Eq. 3.3. Both ρ_1 and ρ_2 have the same definition, for clarity we use $n_0 ... n_3$ as the normalized Stokes parameters for ρ_2. By substituting the definition of the density from Eq. 3.3 into Eq. 3.4, we obtain an expression for the fidelity as a function of the Stokes parameters:

$$F(\rho_1, \rho_2) = \frac{1}{4} \left(\sqrt{\Omega - \sqrt{\omega}} + \sqrt{\Omega + \sqrt{\omega}} \right)^2 \quad \text{with} \tag{3.5}$$

$$\Omega = s_0 n_0 + s_1 n_1 + s_2 n_2 + s_3 n_3 \quad \text{and} \tag{3.6}$$

$$\begin{aligned} \omega =& s_0^2 \left(n_1^2 + n_2^2 + n_3^2 \right) + s_1^2 \left(n_0^2 - n_2^2 - n_3^2 \right) + s_2^2 \left(n_0^2 - n_1^2 - n_3^2 \right) + s_3^2 \left(n_0^2 - n_1^2 - n_2^2 \right) \\ &+ 2 s_0 s_1 n_0 n_1 + 2 s_0 s_2 n_0 n_2 + 2 s_0 s_3 n_0 n_3 + 2 s_1 s_2 n_1 n_2 + 2 s_1 s_3 n_1 n_3 + 2 s_2 s_3 n_2 n_3 \end{aligned} \tag{3.7}$$

This result is valid for both pure and mixed polarization states. However, when the states involved are pure ($S_0^2 = S_1^2 + S_2^2 + S_3^2$) i.e. $p = 1$, the expression of ω in Eq. 3.7 reduces to

$$\omega = \sum_{i=0}^{3} \sum_{j=0}^{3} s_i s_j n_i n_j . \tag{3.8}$$

We now consider several examples illustrating the fidelities between relevant polarization basis states. Specifically, we focus on the three mutually unbiased bases {H,V}, {D,A}, and {R,L}. We choose for ρ_1 the horizontal polarization state H with $s_0 = 1$, $s_1 = 1$, and $s_2 = s_3 = 0$. If ρ_2 is equal to ρ_1 ($\rho_2 = \rho_1$), we naturally find $F(\rho_1, \rho_2) = F(\rho_1, \rho_1) = 1$. If ρ_2 is orthogonal, that is V-polarized, then $n_0 = 1$, $n_1 = -1$ and $n_2 = n_3 = 0$, and we quickly find that the fidelity $F(\rho_1, \rho_2) = 0$, as expected. Finally, if ρ_2 is a basis state in another mutually unbiased basis, for instance diagonally polarized ($n_0 = n_2 = 1$ and $n_1 = n_3 = 0$) it follows that $F(\rho_1, \rho_2) = 1/2$. We summarize:

$$F(\rho_1, \rho_2) = \begin{cases} 1 & \text{for } \rho_1 = \rho_2 \\ 0 & \text{for } \rho_1 \perp \rho_2 \\ 1/2 & \text{for } \rho_1 \text{ and } \rho_2 \text{ basis states of different unbiased bases} \end{cases} \tag{3.9}$$

3.2 Unitary transformation of a long single-mode fiber

In the absence of loss and nonlinear optical effects, within the stationary regime, the polarization transformation by a single-mode fiber is expected to be unitary. This property is crucial for using polarization in quantum communication experiments. Here, we investigate the unitarity of a single-mode fiber experimentally using the setup shown in Fig. 3.2. We use 830 nm laser light (Thorlabs LPS-830-FC) and define its polarization state with a combination of a linear polarizer, a quarter-wave plate, and a half-wave plate before sending it through a 200 m long 780HP single-mode fiber. The polarization state

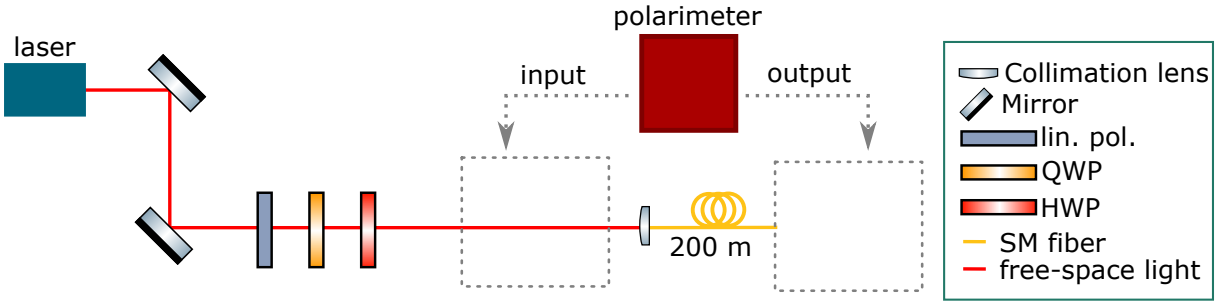


Figure 3.2: Schematic of the experimental setup to measure polarization changes in a 200 m long single-mode optical fiber.

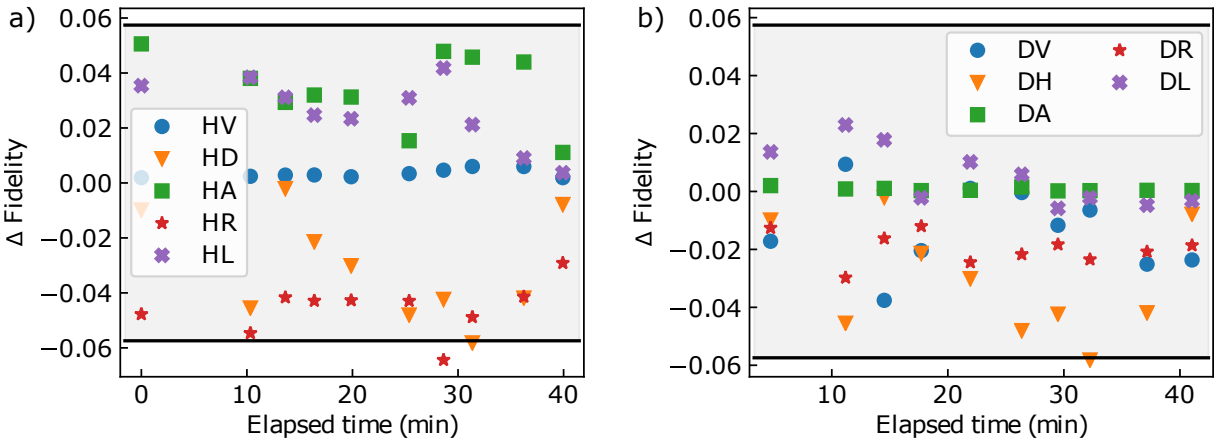


Figure 3.3: The deviation of the measured fidelity after the 200 m fiber from the expected fidelity ΔF as a function of the elapsed time. (a) $\Delta F\left(\rho_{\mathrm{H,out}}, \rho_{i,\mathrm{out}}\right)$ comparing the H and i input polarization states with $i \in \{\mathrm{V,D,A,R,L}\}$. (b) $\Delta F\left(\rho_{\mathrm{D,out}}, \rho_{i,\mathrm{out}}\right)$ comparing the D and i input polarization states with $i \in \{\mathrm{H,V,A,R,L}\}$. The uncertainty caused by imperfect polarization state preparation $\sigma = 0.057$ is indicated by the gray area.

of light is measured using a polarimeter (Thorlabs PAX1000IR1/M), which contains a rotating quarter-wave plate and a linear polarizer. The light is fiber coupled into the polarimeter using the appropriate fiber collimators.

First, we place the polarimeter before the light is coupled into the single-mode fiber ("input" box in Fig. 3.2) and calibrate the angles of the wave plates to obtain the six states of interest H, V, D, A, R, and L. We then send the light through the 200 m long fiber, and measure with the polarimeter the polarization after the fiber output ($\rho_{i,\mathrm{out}}$) by averaging over 5 seconds with a sample frequency of 20 Hz. The input polarization states are permuted in the order H, V, D, A, R, L, and the process is repeated 10 times. We only want to test for unitarity of the fiber transformation, and we are not interested in the absolute output polarization state. Therefore, for every measurement, we calculate the fidelity $F\left(\rho_{j,\mathrm{out}}, \rho_{i,\mathrm{out}}\right)$ of the output polarization states for different input polarizations, and compare to the expected fidelity from Eq. 3.9.

First, we discuss the measured fidelities for horizontal input $F\left(\rho_{\mathrm{H,out}}, \rho_{i,\mathrm{out}}\right)$. The absolute fidelities are expected to be 0 for $i = \mathrm{V}$ and 1/2 for $i \in \{\mathrm{D,A,R,L}\}$. The deviation from these expected fidelities, ΔF, is shown in Fig. 3.3(a) as a function of the duration of the experiment. We observe that most data points lie within the gray region, which

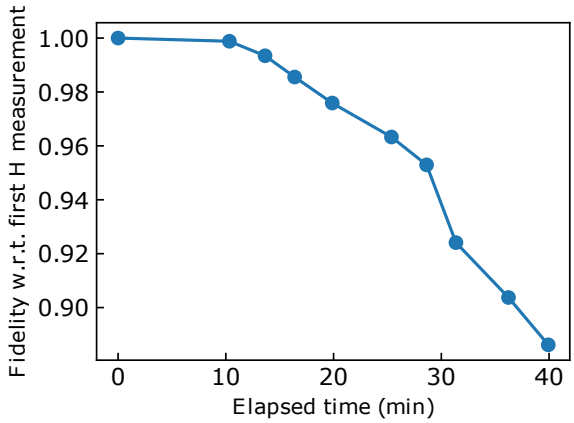


Figure 3.4: Fidelity $F\left(\rho_{\mathrm{H,out}}(0), \rho_{\mathrm{H,out}}(t)\right)$ between polarization states exiting the fiber for an H-polarized input, shown as a function of elapsed time. The fidelity decreases by 11% over a span of 40 minutes.

represents the expected error arising from imperfect preparation of the input polarization states. Since the wave plates are adjusted manually, this error was quantified by repeatedly setting the same input polarization (H), measuring the outcome with the polarimeter, and then readjusting the wave plates. Repeating this process 10 times yielded an expected fidelity error of ± 0.057. The errors of the polarimeter are below 0.25 degrees in both azimuth and ellipticity angles, which results in an inaccuracy of the fidelity of less than 0.0002. We can conclude that, within those errors, the 200 m fiber preserves the unitarity of the polarization states.

Fig. 3.3(b) shows the same analysis as Fig. 3.3(a), except that here the fidelity is calculated with respect to the incident D polarization: ΔF of $F\left(\rho_{\mathrm{D,out}}, \rho_{i,\mathrm{out}}\right)$. We observe a similar result as in Fig. 3.3(a), demonstrating again preservation of unitarity. However, the deviations from the expected fidelity appear smaller than in Fig. 3.3(a), particularly when comparing HR and HL in Fig. 3.3(a) with DR and DL in Fig. 3.3(b). Since the measurements with incident D polarization are performed halfway through each measurement round, the temporal separation between the states used for fidelity calculations differs. The average time between the H and R measurements is 2.8 minutes, while it is only 1.3 minutes between the D and R measurements. These smaller deviations from the expected fidelity in Fig. 3.3(b) suggest a time-dependent change in the polarization transformation of the fibers, which we now proceed to investigate.

Figure 3.4 shows the time-dependent change in fidelity for horizontal input polarization $F\left(\rho_{\mathrm{H,out}}(0), \rho_{\mathrm{H,out}}(t)\right)$, referenced to $t = 0$. We observe an 11% degradation in fidelity over a period of 40 minutes. This decline in fidelity confirms that the difference in spread of ΔF between the measurements in Fig. 3.3(a) and Fig. 3.3(b) can indeed be explained by time-dependent polarization changes.

In conclusion, a long single-mode fiber imposes a unitary transformation on the polarization states of light, as the fidelity between basis states remains unchanged. However, this unitary transformation changes in time, and re-calibration every couple of minutes might be required for experiments that rely on polarization stability.

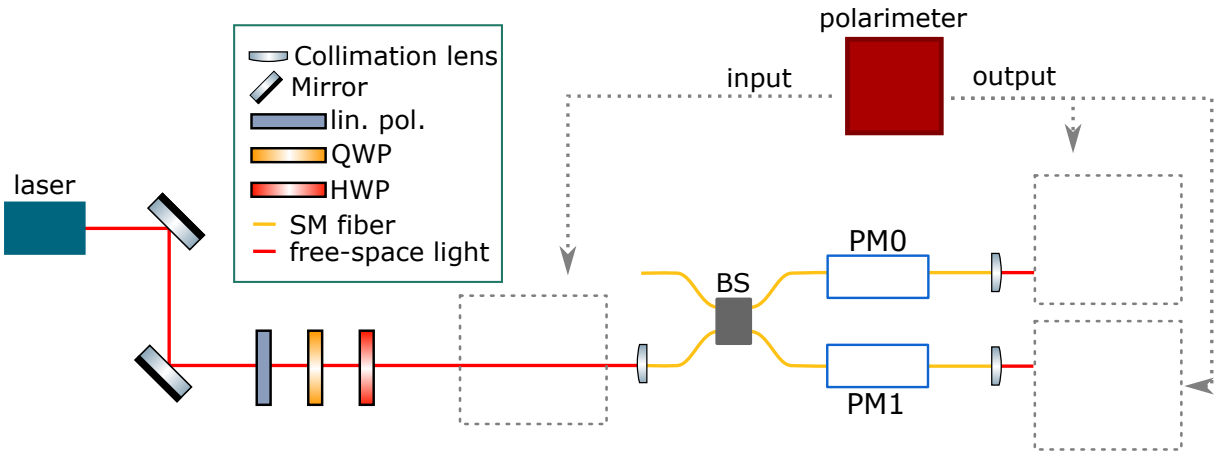


Figure 3.5: Schematic representation of the experimental setup, similar to the setup shown in Fig. 3.2, except that the long single-mode fiber is replaced with a fiber-based 50:50 beam splitter (BS) and two fiber-based polarization modulators (PM0 and PM1).

3.3 Unitary transformation of fiber-based polarization modulators

In a similar way, we investigate now the properties of fiber-based polarization modulators (PolaRITE III from General Photonics Corp.). These modulators are fully fiber-based (and therefore have low loss) and consist of four piezo-electric controlled squeezing actuators. Squeezing the optical fiber changes its birefringence and imposes a similar operation as a wave plate with tunable retardation. In the reference frame of the optical table, the first and third squeezers are oriented at 45°, while the second and fourth squeezers are aligned horizontally. Combined, the four squeezers enable full control of the output polarization state; any pure polarization state can be transformed into any other pure polarization state.

As with the long single-mode fiber discussed in Section 3.2, we first test whether the polarization modulators apply a unitary transformation to the polarization state of light. A similar experimental setup is used, shown in Fig. 3.5. The main difference is that the 200 m fiber is replaced with a non-polarizing 50:50 fiber-based beam splitter (Thorlabs TW850R5A2), with a polarization modulator (PM0 and PM1) positioned at each output to enable testing of the two modulators. The light exiting the polarization modulators is coupled into free space to allow the polarimeter to be inserted without disturbing the optical fibers in the setup. In addition, all fibers were secured to the optical table to prevent accidental movement, and a waiting period was introduced between setup and measurement to allow for relaxation. The measurement procedure is similar to the one discussed in Section 3.2. The input states (H,V,D,A,R,L) are adjusted in the same manner. We now change the voltage over the first squeezer from 0 to 5 V in steps of 0.05 V for each of the input states, and for each voltage step, the polarization state is averaged over 1 second at a frequency of 10 Hz with a total measurement time of around 2 minutes per polarization setting. We calculate the fidelities and average over the voltage. Fig. 3.6 shows for PM0 (a) and PM1 (b) the difference in measured fidelity $F\left(\rho_{i,\mathrm{out}}(U), \rho_{j,\mathrm{out}}(U)\right)$ from the expected fidelity for input states i and j. Note that the case of $i = j$ is excluded

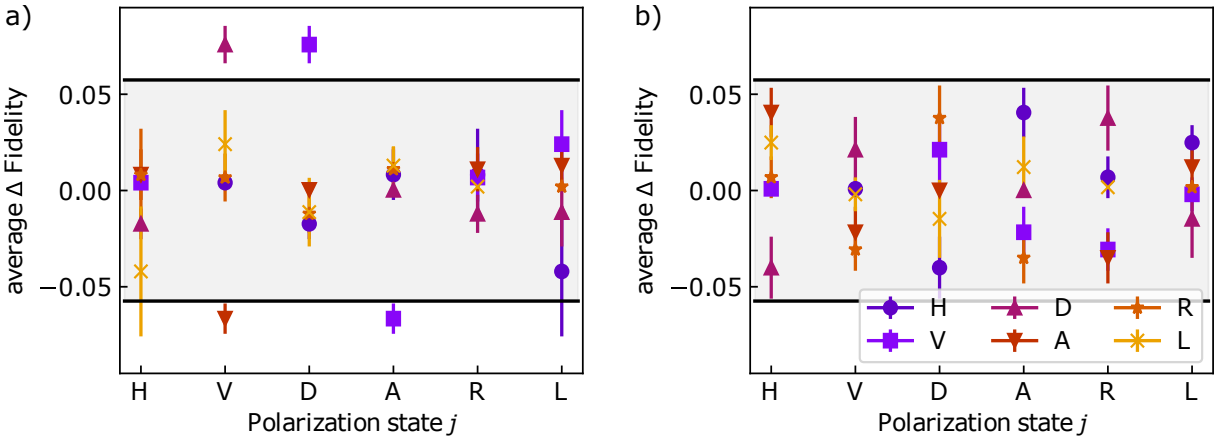


Figure 3.6: Deviation of the fidelity $F\left(\rho_{i,\mathrm{out}}(U), \rho_{j,\mathrm{out}}(U)\right)$ between input state i and j from the expected fidelity, averaged over the squeezer voltage and for polarization modulator PM0 (a) and PM1 (b). The input polarization state j is indicated on the x-axis, and the markers indicate state i. The error bars show the statistical experimental errors from the polarization measurements, and the gray area indicates the expected error by the manual setting of the input polarization states.

as it results in $\Delta F = 0$. We see again that most measurements fall within the expected error range.

To conclude, by comparing the fidelity of the measured output states with the expected fidelities, we found that the squeezer-based polarization modulators induce unitary operations in polarization space, for any voltages applied to the squeezers.

3.4 Stability of fiber-based polarization modulators

To measure the temporal stability of our polarization modulators, we use the same setup as shown in Fig. 3.5. Instead of changing the voltage on a single squeezer, we now first apply a static voltage to two, three, or all four of the squeezers. After applying the voltage, the polarization state behind each polarization modulator is measured for a total time of 300 s in steps of 0.048 s. The squeezer voltages are set such that the polarimeter detects either horizontal (H) or vertical (V) polarized light. Although using all four squeezers allows full control of the output polarization state, H and V polarization can be reached with only two or three squeezers, if a suitable polarization state is chosen at the input of the modulator.

The results are presented in Fig. 3.7, which shows the change in measured fidelity $(F\left(\rho_i(0), \rho_i(t)\right))$ relative to the first measurement point $(F = 1)$ for both modulators. From these results, we observe an overall change in fidelity below a percent, 0.5% in the worst case, over a span of five minutes for PM0. For PM1, if 2 or 3 squeezers are used, the deviation in fidelity is similar to that of PM0, but when all four squeezers are in operation, the change in fidelity reaches a few percent.

Finally, we investigate the temporal evolution of polarization overlap between the two polarization modulators, a scenario directly relevant to the implementation of a two-photon QPV protocol. As before, we evaluate the fidelity of the measured polarization

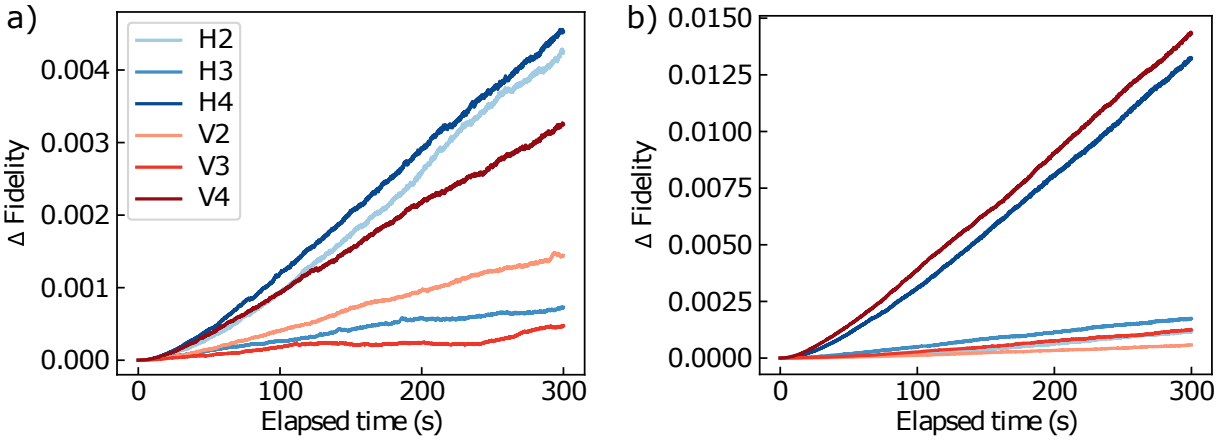


Figure 3.7: Deviation of the fidelity $F\left(\rho_i(0), \rho_i(t)\right)$ from perfect polarization state overlap ($F = 1$) as a function of the elapsed time t for $i = \{\mathrm{H}, \mathrm{V}\}$ polarization, created with 2, 3, or 4 squeezers, for PM0 (a) and PM1 (b). The labels is indicate the polarization state i and the number of used squeezers s, for example, $i = \mathrm{H2}$ means H-polarized light created using 2 squeezers.

states with respect to their expected values, but now for light exiting both PM0 and PM1 simultaneously. Fig. 3.8 shows the deviation of the fidelity $F\left(\rho_i(0), \rho_j(t)\right)$ from the expected fidelity, where labels ijs indicate the combinations of input polarization states i, j, and the number of squeezers used s (which is the same for PM0 and PM1). Fig. 3.8(a) shows results for parallel polarization states with expected maximum overlap ($F = 1$), while Fig. 3.8(b) shows the results for orthogonal states (with expected overlap $F = 0$).

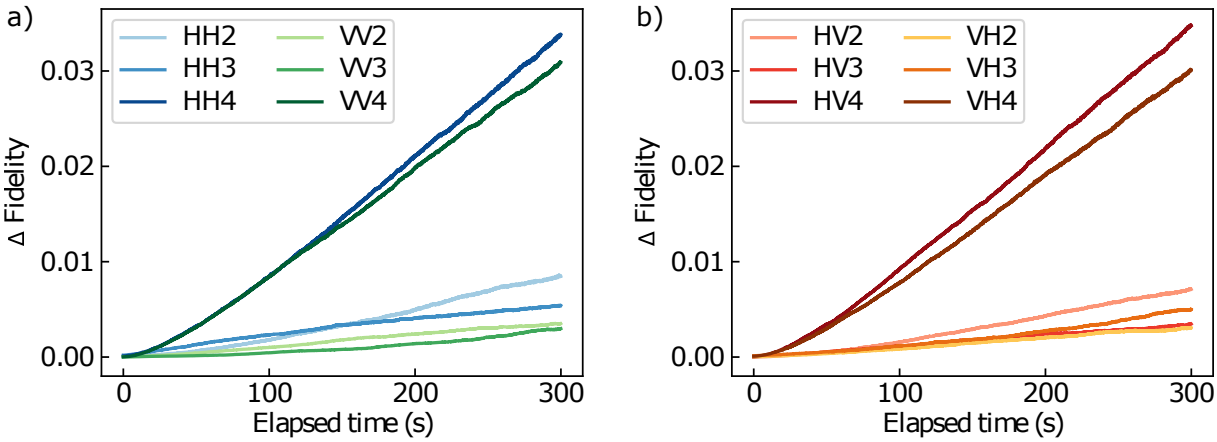


Figure 3.8: Deviation of the measured fidelity $F\left(\rho_i(t), \rho_j(t)\right)$ from the expected fidelity as a function of time, for the case of equal polarization (a) where $F = 1$ is expected and orthogonal polarization (b) where $F = 0$ is expected.

We observe that the change in fidelity in Fig. 3.8 is larger than the shift in fidelity for each modulator individually in Fig. 3.7. This is expected, since the polarization changes of both modulators are independent, and this can lead to larger changes of fidelity. Fig. 3.8 shows that using all four squeezers generally results in the worst overlap between the states created by PM0 and PM1. This observation is corroborated by the fact that, particularly for PM1, this configuration exhibits the largest shift in fidelity over time, whereas using

three of the four squeezers produces a much smaller shift of approximately 1% over a 5-minute span. From these observations, we conclude that using three of the four squeezers generally provides the optimal static stability of the polarization states over prolonged periods, and using all four squeezers results in the poorest stability. However, it should be noted that the fourth squeezer may be necessary to prepare a desired polarization state.

3.5 Long term polarization fluctuations in a 200 m long single-mode fiber

Since a QPV demonstration experiment might run over several hours, we now investigate fiber-induced polarization changes over long periods of time, using the same experimental setup as shown in Fig. 3.2. Eight overnight measurements were taken over a span of 18 days, each having a duration of approximately 15 hours, and measurements were taken each 50 ms (day 1), 0.5 s (days 2, 3, and 9), and 1 minute. For the last five measurements, the lab temperature was recorded simultaneously using a Conrad TFD 128 temperature logger with an accuracy of 0.1 °C, positioned next to the optical fiber.

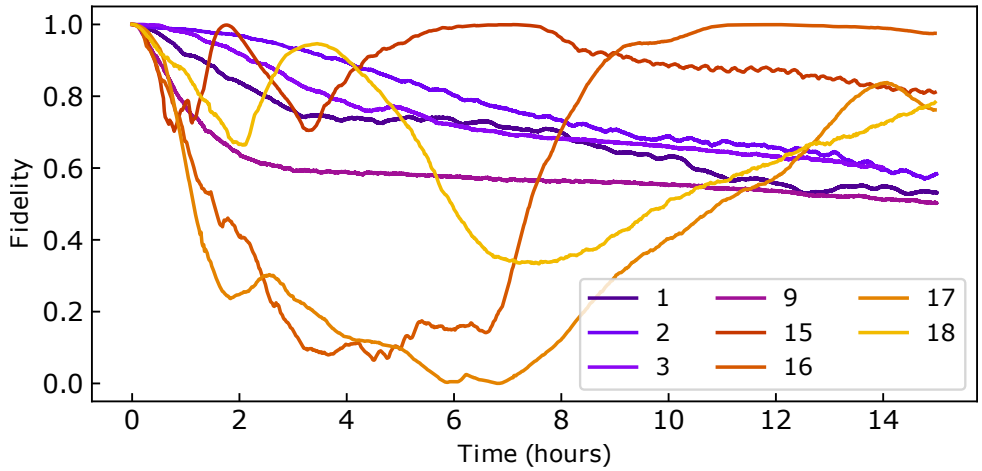


Figure 3.9: Polarization state fidelity $F(\rho_i(0), \rho_i(t))$ as a function of elapsed time t in hours measured over different nights in the span of 18 days (i).

Fig. 3.9 shows the evolution of the polarization state fidelity with respect to the polarization state at the start of the measurement. For the first four measurements (days 1-9), the fidelity decreases gradually towards approximately 0.5. In the final four measurements (days 15-18), the fidelity exhibits stronger fluctuations without a clear trend. This behavior cannot be attributed to fiber relaxation processes, since in that case the rate of change in fidelity would be expected to slow over time.

To investigate the unexpected fluctuations in fidelity in more detail, we focus on measurements taken on days 9 and 16. Fig. 3.10(a) and (b) show the evolution of the fidelity on these days, along with the corresponding state evolution on the Poincaré sphere. We observe that for day 9 the polarization state moves away from the initial point, first quickly and then more slowly, while for day 16 the polarization first moves away from the initial state but later returns to it. This becomes clearer in Fig. 3.10(c) and (d), where we show the velocity of the polarization state changes on the Poincaré sphere. We also show the measured lab temperature, and although the temperature changes are rather small in

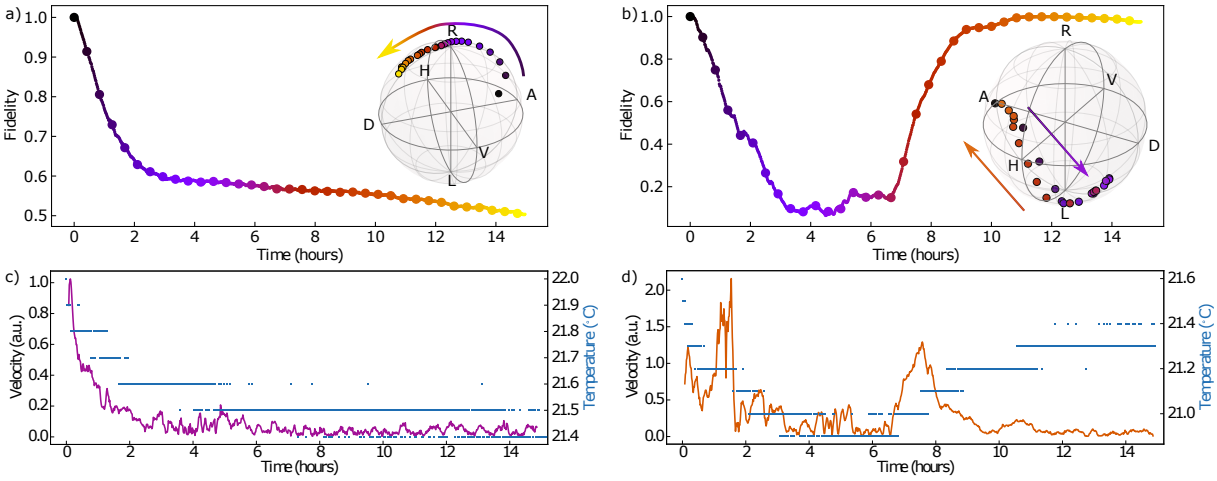


Figure 3.10: Fidelity $F\left(\rho_i(0), \rho_i(t)\right)$ as a function of the elapsed time t for day $i = 9$ (a) and day $i = 16$ (b), the circular markers indicate points that are also shown on the Poincaré sphere in the inset, the arrow indicates the temporal evolution. Panels (c, day 9) and (d, day 16) show for the velocity of the polarization changes on the Poincaré sphere and the lab temperature measured simultaneously.

the order of 0.1 °C, we observe a clear correlation between temperature and polarization changes. We note that the initial relatively rapid changes in temperature and polarization are most likely caused by personnel leaving the laboratory.

Our results highlight the importance of temperature stabilization, but they also show that recalibrating the polarization, for example every 10 minutes, is sufficient to mitigate temperature-induced effects. The origin of these temperature-dependent polarization drifts has been investigated before and is most likely due to changes in strain in the optical fiber, which in turn modifies the strain-induced birefringence of said fiber [44].

3.6 Polarization mode dispersion in fibers

Polarization mode dispersion (PMD) describes a possible polarization-dependent group velocity of light during propagation in an optical fiber. If it is significant, it can pose serious limitations on using polarization qubits in quantum network protocols [45]. It is a frequency-dependent phenomenon that arises in fibers due to imperfections, stress, or geometrically induced birefringence such as a non-circularity of the fiber core, leading to distortion of propagating optical pulses [46].

To measure the PMD of our fiber, we use a so-called Müller matrix method (MMM) [47, 48] to determine the differential group delay (DGD) caused by PMD. In this method, two polarization input states are used to reconstruct the rotation matrix describing the polarization change by the optical fiber for two different optical frequencies ω_0 and $\omega_0 + \Delta\omega$. From this rotation matrix, the rotation angle is extracted, which in turn is used to calculate the DGD. We use vertical and anti-diagonal polarization as input states, which are described by the Stokes vectors $\vec{t}_{\mathrm{V}}$ and $\vec{t}_{\mathrm{A}}$. In the experiment shown in Fig. 3.11, we prepare these states simply by using a linear polarizer in a computer-controlled rotation actuator. As the light source, we use a narrow-linewidth frequency-tunable continuous

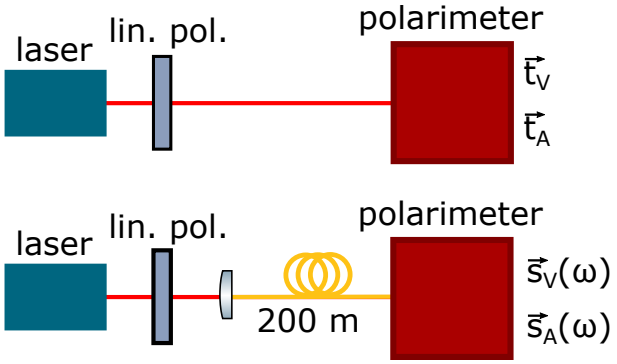


Figure 3.11: Schematic representation of measuring the input state $\vec{t}_V, \vec{t}_A$ (top) and output states $\vec{s}_V(\omega), \vec{s}_A(\omega)$ (bottom) behind a 200m long 780HP optical fiber as a function of the wavelength of the frequency tunable continuous wave laser using a polarimeter.

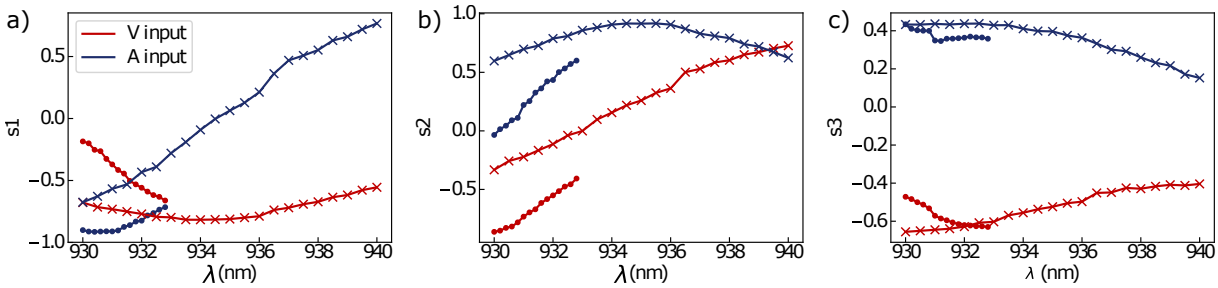


Figure 3.12: Normalized stokes parameters s_1(a), s_2(b) and s_3(c) as a function of the optical wavelength λ, for vertically (red) and anti-diagonally (blue) polarized input light for measurement 1 (●) and measurement 2 (×).

wave laser at around $\lambda = 930$ nm. We measure the polarization state at the output of the 200 m long 780 HP single-mode fiber using a polarimeter and obtain the Stokes vectors $\vec{s}_V(\omega)$ and $\vec{s}_A(\omega)$ for frequency ω. We discuss two measurements performed on consecutive days, where in measurement 1, the wavelength was tuned from 930.0 to 933.0 nm in steps of 0.2 nm, and in measurement 2, the wavelength was changed from 930.0 to 940.0 nm in steps of 0.5 nm. The optical wavelength was recorded using a spectrometer. For each wavelength and input polarization setting, the output polarization was averaged over approximately 5 seconds at a sampling frequency of 21 Hz. For each wavelength, the total measurement time, including changing of the laser frequency and polarizer adjustment, usually takes less than a minute, resulting in a total measurement time of 27 minutes for measurement 1 and 39 minutes for measurement 2.

Fig. 3.12 shows the wavelength-dependent normalized Stokes parameters calculated from the measured azimuth and ellipticity angles. We see that all three Stokes parameters experience a significant change over the measured wavelength range. We calculate the output Stokes vectors $\vec{s}_V(\omega)$ and $\vec{s}_A(\omega)$ from the Stokes parameters and use the Müller matrix method to calculate the differential group delay (DGD). First, for two laser frequencies ω and $\omega + \Delta\omega$, we calculate the polarization rotation matrices R that relate the output to the input polarization by $\vec{t} = R \cdot \vec{s}$ with a trick described by Jopson et al. [47], only requiring 2 input polarization states. Now we can calculate the difference rotation matrix that relates the output Stokes vectors at the two frequencies (the transpose of a

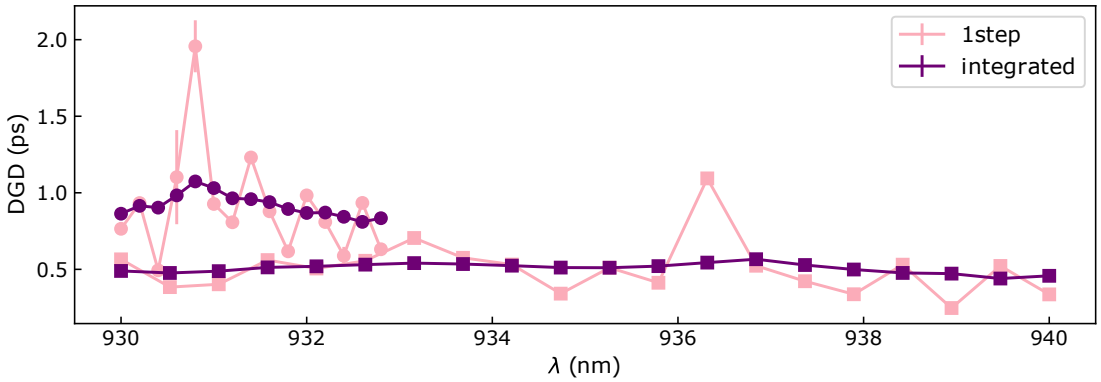


Figure 3.13: Differential group delay (DGD) as a function of the optical wavelength calculated using both the 1-step (pink) and integrated (purple) method. The DGD was calculated for both measurement 1 (●) and measurement 2 (■).

rotation matrix results in reversed rotation):

$$R_\Delta = R_{\omega+\Delta\omega} R_\omega^T \tag{3.10}$$

From R_Δ, we obtain the rotation angle ϕ from $\cos\phi = \frac{1}{2}(\mathrm{Tr}R_\Delta - 1)$, and finally we obtain the DGD:

$$\Delta\tau = \frac{\phi}{\Delta\omega} \tag{3.11}$$

The experimentally obtained DGD is shown in Fig. 3.13 as a function of the optical wavelength λ, for both measurements. The DGD was calculated for neighboring measurements at ω and $\omega + \Delta\omega$ ("1 step") or by calculating the DGD at ω with respect to every other frequency in the measurement and subsequent averaging over all values ("integrated"). The "integrated" method shows fewer variations due to the averaging.

The average DGD is 0.91 ± 0.05 ps (1-step method) and 0.92 ± 0.01 ps (integrated method) for measurement 1, and 0.503 ± 0.009 ps (1-step method) and 0.507 ± 0.002 ps (integrated method) for measurement 2. A possible explanation of this discrepancy is that the measurements were performed on two consecutive days, and it is known that environmental factors easily change the measured DGD [49, 50]. To compare to literature data, we determine the PMD coefficient in units of ps/$\sqrt{\text{km}}$. This square-root length dependence originates in the fact that, in long fibers, different sections contribute in an uncorrelated way to the DGD. We obtain PMD coefficients of this fiber using the average DGD: 2.0 ± 0.1 ps/$\sqrt{\text{km}}$ (1-step method) and 2.06 ± 0.02 ps/$\sqrt{\text{km}}$ (integrated method) for measurement 1, and 1.12 ± 0.02 ps/$\sqrt{\text{km}}$ (1-step method) and 1.134 ± 0.007 ps/$\sqrt{\text{km}}$ (integrated method) for measurement 2. These PMD coefficients do fit within the broad range of values that can be found in literature [45, 47, 51–54].

Even if we consider the worst-case scenario for our 200 m fiber (DGD $\approx$ 2 ps), the broadening of the optical pulses is very small compared to the single-photon wavepacket lengths used in our experiments (around 50-100 ps). For longer fibers, however, PMD effects become relevant, for instance for a 10 km long fiber one can expect around 5 ps PMD, which would significantly decohere the polarization qubits and would require active stabilization [55, 56].

4 Hong-Ou-Mandel interference in a realistic unbalanced Mach-Zehnder interferometer

To characterize the indistinguishability of quantum-dot-based and other single-photon sources, often, sequential photons are interfered in an unbalanced Mach-Zehnder interferometer, where Hong-Ou-Mandel two-photon quantum interference is used to determine the single-photon indistinguishability. However, these photon correlations contain more information than just the single-photon indistinguishability, in particular if two-photon correlation events occur with time delay $\Delta\tau$ equal to the internal delay t_d of the interferometer. We give here a didactic description and derivation of those correlations at $\Delta\tau = \pm t_d$, and derive an expression of the photon indistinguishability for the generic case of imperfect beam splitters and other experimental imperfections. We validate our theory by comparison to literature and to experimental measurements with photons produced by a InGaAs/GaAs quantum dot – microcavity single-photon source.

4.1 Introduction

High single-photon indistinguishability is an important requirement for most applications quantum optics that rely on two-photon Hong-Ou-Mandel (HOM) interference, including linear optical quantum computing and quantum networks [57–59]. To characterize the photon indistinguishability of a source, it is common to use an unbalanced Mach-Zehnder interferometer (MZI) [60–65], in which consecutive single photons are probabilistically split by the first beam splitter, synchronized with later photons via a time delay, and then made to interfere at the second beam splitter. Depending on their mutual indistinguishability, or equivalently the overlap of their wave functions across all degrees of freedom, HOM interference leading to photon bunching may or may not occur. This effect can be readily observed using two single-photon detectors at the output of the second beam splitter.

The measured photon correlations at zero time delay provide a measure of the degree of indistinguishability of the single-photon source. These measurements can also be done for delays much larger than the time between consecutively produced single-photons in order to probe decoherence of the single-photon source on longer time-scales [66, 67].

For both short and long delays, the measured two-photon correlations exhibit features not only at zero time delay but also at a delay equal to the path length difference of the interferometer [66, 68]. These additional features have recently been shown to contain information about the photon-number coherence of the source [69, 70], but they also appear for perfect single-photon sources without photon-number coherence. In the first part of this chapter, we give an intuitive qualitative explanation of these features and correlations. Moreover, most existing analyses assume an idealized, perfectly symmetric (balanced in intensity) MZI, which is often not the case.

To address these challenges, we first dive deeper into the cause of the additional features in the correlation measurements. We then develop a comprehensive analytical framework that describes two-photon interference in an MZI as a function of all relevant experimental parameters, including intensity imbalance in the interferometer and experimental errors in the wavefunction overlap which is tuned by the polarization state of the photons. We validate our analytical framework by comparison to literature and to two-photon correlation measurements performed with our quantum dot – microcavity single-photon source [71, 72].

4.2 Theory

A two-photon correlation measurement using an MZI is presented in Fig. 4.1, where the measured coincidence counts are shown as a function of the time delay $\Delta\tau$ between detection events. The three different colors represent three different regimes of correlations: red are the correlations corresponding to the two detectors clicking simultaneously ($\Delta\tau = 0$), purple corresponds to $\Delta\tau = \pm t_d$ the delay in the MZI which is here equal to the temporal separation of the single-photon wavepackets τ_l, and blue are other correlations. We clearly observe that the purple coincidence peaks are lower than the blue ones, and the red peak is even lower. This latter is a signature of HOM photon bunching, where two photons predominantly exit the final beam splitter "bunched" together and result in reduced coincidences.

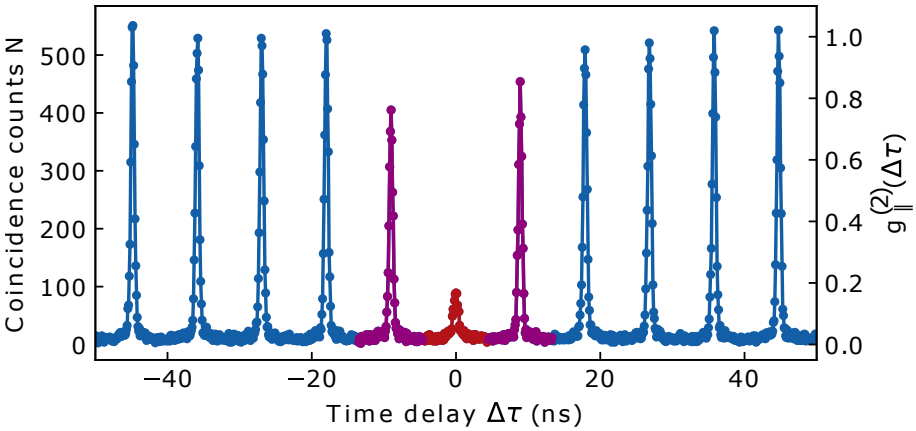


Figure 4.1: Example of a two-photon correlation measurement as a function of the time delay between detection events to determine the indistinguishability of a quantum dot single-photon source. The left axis shows the raw coincidence counts and on the right axis we show the normalized $g^{(2)}$. For this particular example, the delay in the Mach-Zehnder interferometer is equal to the pulse period of $\tau_l = 9$ ns. The three different colors represent three different regimes of correlations: red are the correlations corresponding to the two detectors clicking simultaneously ($\Delta\tau = 0$), purple corresponds to $\Delta\tau = \pm t_d$ the delay in the MZI, and blue are all other correlations.

4.2.1 The ideal Mach-Zehnder interferometer

First we explain in detail why the correlations at $\Delta\tau = \pm t_d$ are lower than all other $\Delta\tau \neq 0$ correlations. To simplify the explanation we assume that the MZI is ideal, i.e. has perfectly balanced splitting ratios and equal transmission in both interferometer arms. Furthermore, we set the delay between the short and long arm of the interferometer t_d to be equal to the time between two consecutive photons in the single-photon stream τ_l, as is the case for the measurement shown in Fig. 4.1. A schematic of this simplified MZI is shown in Fig. 4.2(a) consisting of two beam splitters (BS_1, BS_2) and two single-photon detectors (D1, D2). The numbers (1), (2) and (3) denote different locations in the interferometer for which we show a cartoon of the single-photon stream in Fig. 4.2(b). (1) is before the first beam splitter BS_1, (2) is just after splitting the single-photon stream and (3) is after temporal synchronization before the photons interfere at BS_2.

Before entering the interferometer (1) there is a stream of single-photons (●) separated by τ_l. In this example we only describe the photon statistics with respect to the photon depicted by blue dot ● in the stream. After the 50:50 beam splitter (2) the photons are in superposition between the two arms of the interferometer (○) and after the delay (3), the photons in the long arm of the interferometer are delayed by t_d, which in this case is equal to the temporal separation of the photons τ_l. Now we have to distinguish two cases of photon trajectories: one where the photon ● went through the short arm of the interferometer and another where it went through the long arm. If the photon went into the short arm, there has to be an empty time bin at $+t_d$ in the long arm, because this is where the photon would have been if it had taken the longer path. Similarly, if the photon went into the the long path there has to be an empty time bin at $-t_d$ in the short arm. Consequently, there is always one trajectory less that leads to a coincidence detection at $\pm t_d$ time delay compared to all other non-zero delays. Because there are generally four

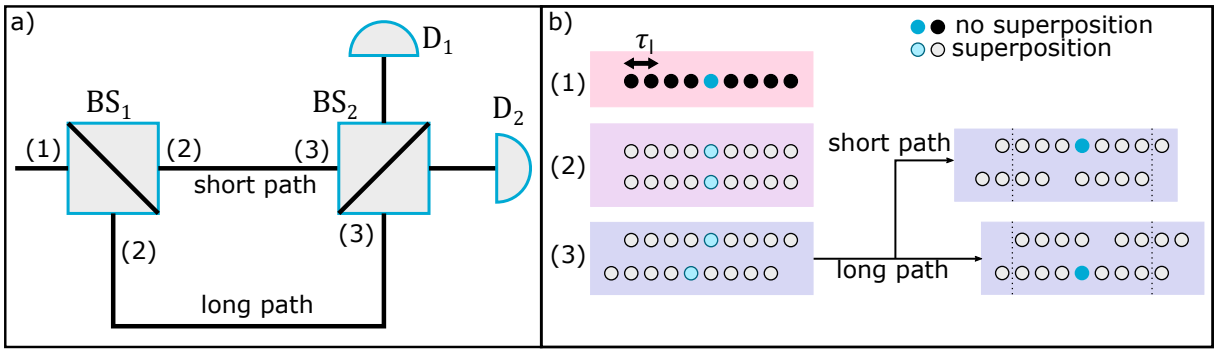


Figure 4.2: Ideal Mach-Zehnder interferometer and photon correlations. (a) schematic of the MZI, (b) cartoon of the photon streams before the first beam splitter (1), just after the first beam splitter (2) and after the temporal delay in the lower arm (3), where the delay τ_d between the arms is equal to the time between consecutive photons τ_l. A blue color indicates an arbitrarily chosen photon, and upper/lower streams indicate upper/lower paths. Empty circles indicate photons in superposition between different paths.

possible photon trajectories that lead to coincidence detection at non-zero time delay, the peaks corresponding to $\pm t_d$ have a height of 3/4 instead of 1.

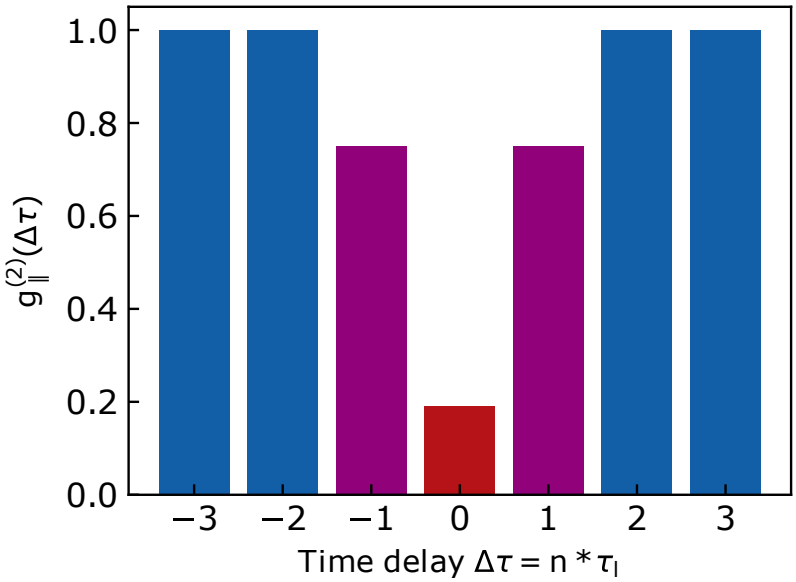


Figure 4.3: Theoretical correlations in the simplified MZI where the red bar corresponds to zero time-delay correlations indicating imperfect indistinguishability as present in the experimental data in Fig. 4.1, the purple bars corresponds to correlations at time differences equal to the time delay of the MZI arms, and all other correlations are shown in blue. The detection time delay $\Delta\tau$ is shown as integer multiples of the period between two consecutive photons in the initial single-photon stream, $n \cdot \tau_l$.

We visualize this result in Fig. 4.3, where the normalized $g^{(2)}(\Delta\tau)$ is shown for this particular example. The red bar at $\Delta\tau = 0$ is set to match with the experimental value shown in Fig. 4.1 and is absent for perfectly indistinguishable photons. However, we

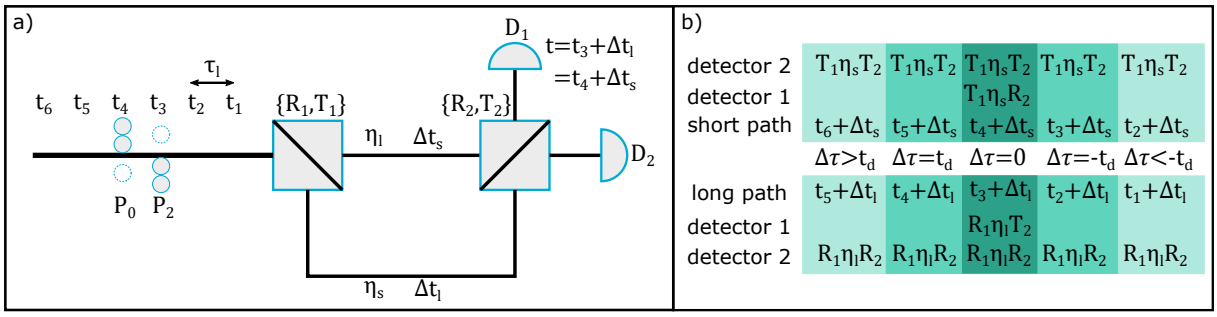


Figure 4.4: A realistic Mach-Zehnder interferometer. (a) Schematic representation of the interferometer with imperfect beam splitters with reflectivity R and transmission T, and finite transmission through the interferometer arms η. (b) shows time bins and possible photon trajectories, including which experimental parameters the photons experience.

note that the explanation of correlations at $\Delta\tau = \pm t_d$ (purple) is independent on the photon indistinguishability or wavefunction overlap of the photons since the detection events do not occur simultaneously and hence no interference effects take place (if there is not photon-number coherence).

We see that the purple side-peaks at $\Delta\tau = \pm t_d$ of our experimental results in Fig. 4.1 deviate from the theoretical prediction in Fig. 4.3, the height of the peaks surpass 0.75 and are not equal. Furthermore, we observe that the peaks for $|\Delta\tau| > t_d$ are not exactly equal to one and fluctuate. The latter can be explained by shot noise caused by non-ideal photon generation and detection. The former is caused by imperfections in the Mach-Zehnder interferometer as we will show now.

4.2.2 A realistic Mach-Zehnder interferometer

Parameters and assumptions

A schematic representation of a realistic Mach-Zehnder interferometer is shown in Fig. 4.4. At the input of the interferometer, we consider a photon stream with six time bins $t_1 ... t_6$. For each time bin, we describe the photonic state by an incoherent mixture of zero, one, and two photons using the density matrix $\rho = P_0|0\rangle\langle 0| + P_1|1\rangle\langle 1| + P_2|2\rangle\langle 2|$, where P_0, P_1 and P_2 are the probabilities of 0, 1 or 2 photons. We assume that these probabilities do not change with time and that the single-photon source exhibits low brightness such that: $P_0 \gg P_1 \gg P_2$ with $P_0 \approx 1$. The first beam splitter of the interferometer (BS_1) distributes the photon stream over the arms of the MZI, in the shorter arm they experience a temporal delay of Δt_s with a transmission of η_s, and in the longer arm a delay of Δt_l with transmission η_l. The temporal delay between the two arms t_d is set, in this example, to the time difference between two consecutive photons τ_l, i.e., $t_d = \tau_l = \Delta t_l - \Delta t_s = t_4 - t_3$. The second beam splitter (BS_2) recombines the two arms of the interferometer, and detectors D1 and D2 are used for coincidence detection.

Without restricting generality, we now only take correlations into account with respect to a detection event of D1 at time t where $t = t_3 + \Delta t_l = t_4 + \Delta t_s$, meaning that it was caused either by a photon created at time t_3 which had taken the long arm of the interferometer (probability $P_1 R_1 \eta_l$) or a photon that was created at t_4 that had taken the short path (probability $P_1 T_1 \eta_s$). In order to result in a detection event by detector

D1, a photon from the short path should be reflected by BS_2 (R_2) or transmitted (T_2) if the photon came from the long path. To describe these photon trajectories we use the following notation:

$$\begin{aligned}(t_3 + \Delta t_l)_{D1} &: P_1 R_1 \eta_l T_2 \\ (t_4 + \Delta t_s)_{D1} &: P_1 T_1 \eta_s R_2\end{aligned} \tag{4.1}$$

These photon trajectories are also depicted in Fig. 4.4(b).

We now calculate the correlations as a function of the detection time difference $\Delta\tau$ and now consider three different cases: In the first case, both detectors click simultaneously ($\Delta\tau = 0$), the second one is where the delay between click events is equal to the delay between the arms of the MZI ($\Delta\tau = \pm t_d$) and the last case are the correlations for all other $\Delta\tau$. In the particular example given in Fig. 4.4 we consider the last case to be $\Delta\tau = \pm 2t_d$; this choice has no influence on the outcome of the discussion.

Uncorrelated coincidences at $\Delta\tau = \pm 2t_d$

These coincidences are used for normalization of the second-order correlation function. For now we focus only on the case where detector D2 clicks after D1. As shown in Fig. 4.4(b), there are two options that lead to a click at detector D2 at a time difference of $\Delta\tau = 2t_d$, namely a photon created at t_5 taking the long arm and a photon created at time t_6 taking the short arm. However, the operation by the second beam splitter is now mirrored, since states moving through the short arm now need to be transmitted by the second beam splitter to arrive at D2 and reflected if they traveled through the longer arm. These two possible options for D2 in combination with the two options for a click at time t by D1 results in four contributing terms:

$$\begin{aligned}(t_3 + \Delta t_l)_{D1}\,(t_5 + \Delta t_l)_{D2} &: P_1^2 R_1^2 \eta_l^2 T_2 R_2 \\ (t_3 + \Delta t_l)_{D1}\,(t_6 + \Delta t_s)_{D2} &: P_1^2 R_1 \eta_l T_1 \eta_s R_2^2 \\ (t_4 + \Delta t_s)_{D1}\,(t_5 + \Delta t_l)_{D2} &: P_1^2 T_1 \eta_s R_1 \eta_l T_2^2 \\ (t_4 + \Delta t_s)_{D1}\,(t_6 + \Delta t_s)_{D2} &: P_1^2 T_1^2 \eta_s^2 T_2 R_2\end{aligned} \tag{4.2}$$

The total uncorrelated coincidences probability $A_\pm$ is the sum of the four contributions:

$$A_\pm = P_1^2 \left\{ R_2 T_2 \left(R_1^2 \eta_l^2 + T_1^2 \eta_s^2 \right) + T_1 \eta_s R_1 \eta_l \left(T_2^2 + R_2^2 \right) \right\} \tag{4.3}$$

The case where $\Delta\tau = -2t_d$, detector D2 clicks before D1 does, follows the same reasoning and results in the exact same expression.

Reduced coincidences at $\Delta\tau = \pm t_d$

In order to calculate the correlations at $\Delta\tau = t_d = \Delta t_l - \Delta t_s$, we again first only consider a positive delay where D1 clicks before D2 does, which again consists of four contributions:

$$\begin{aligned}(t_3 + \Delta t_l)_{D1}\,(t_4 + \Delta t_l)_{D2} &: P_1^2 R_1^2 \eta_l^2 R_2 T_2 \\ (t_4 + \Delta t_s)_{D1}\,(t_5 + \Delta t_s)_{D2} &: P_1^2 T_1^2 \eta_s^2 R_2 T_2 \\ (t_3 + \Delta t_l)_{D1}\,(t_5 + \Delta t_s)_{D2} &: P_1^2 R_1 \eta_l T_1 \eta_s T_2^2 \\ (t_4 + \Delta t_s)_{D1}\,(t_4 + \Delta t_l)_{D2} &: P_1^2 g^{(2)}(0) R_1 \eta_l T_1 \eta_s R_2^2\end{aligned} \tag{4.4}$$

The first three terms of Equation 4.4 are similar in nature to the four contributions for the previous regime where $\Delta\tau = \pm 2t_d$ (Eq. 4.2). However, the last term can only occur if two photons are created at time t_4 and that move through opposite arms of the interferometer. Under the assumption that a maximum of two photons are distributed over the six possible time bins, we can describe this multi-photon component in two time bins by P_0P_2. Under the assumptions the photon statistics of the source does not change over time, and a low brightness in combination with the expression for the Hanbury Brown and Twiss (HBT) second-order correlation function $g^{(2)}(0) = \frac{2P_2}{(P_1+2P_2)^2}$ we can state that $P_2P_0 \approx \frac{1}{2}g^{(2)}(0)P_1^2$. Furthermore, since it does not matter which of the two photons enters which path, as long as they take opposite arms of the interferometer, we gain an additional factor 2 resulting in the expression seen in the last term of Equation 4.4.

This means that for $\Delta\tau = t_d$ we obtain for the total coincidence probability

$$A_{t_d} = P_1^2 \left\{ R_2T_2 \left(R_1^2\eta_l^2 + T_1^2\eta_s^2 \right) + R_1\eta_l T_1\eta_s \left(T_2^2 + g^{(2)}(0)R_2^2 \right) \right\}. \tag{4.5}$$

Similarly, we can derive the expression for coincidences at $\Delta\tau = -t_d$ where D2 clicks before D1 and obtain

$$A_{-t_d} = P_1^2 \left\{ R_2T_2 \left(R_1^2\eta_l^2 + T_1^2\eta_s^2 \right) + T_1\eta_s R_1\eta_l \left(g^{(2)}(0)T_2^2 + R_2^2 \right) \right\}. \tag{4.6}$$

The reason why the multi-photon contribution has moved to the T_2^2 term is that this contribution belongs to the term $(t_3 + \Delta t_l)_{D1}(t_3 + \Delta t_s)_{D2}$ which requires both photons to be transmitted by the second beam splitter.

Coincidences at $\Delta\tau = 0$

Finally, we discuss the case that detectors D1 and D2 are clicking simultaneously. Following an analogous procedure as before we obtain 4 contributions:

$$\begin{aligned} &(t_3 + \Delta t_l)_{D1}(t_3 + \Delta t_l)_{D2} \\ &(t_4 + \Delta t_s)_{D1}(t_4 + \Delta t_s)_{D2} \\ &(t_3 + \Delta t_l)_{D1}(t_4 + \Delta t_s)_{D2} \\ &(t_4 + \Delta t_s)_{D1}(t_3 + \Delta t_l)_{D2} \end{aligned} \tag{4.7}$$

The first two contributions stem from two photons created in the same time bin which traveled through the same arm of the interferometer, arriving at different detectors. Hence, they can be written in a similar way to the multi-photon component derived for the case $\Delta\tau = \pm t_d$:

$$\begin{aligned} &(t_3 + \Delta t_l)_{D1}(t_3 + \Delta t_l)_{D2} : g^{(2)}(0)P_1^2R_1^2\eta_l^2R_2T_2 \\ &(t_4 + \Delta t_s)_{D1}(t_4 + \Delta t_s)_{D2} : g^{(2)}(0)P_1^2T_1^2\eta_s^2R_2T_2 \end{aligned} \tag{4.8}$$

The last two terms in Eq. 4.7 imply that one photon was created at time t_3 and the other at time t_4. Naively one would use the same method as for $\Delta\tau = \pm 2t_d$:

$$\begin{aligned} &(t_3 + \Delta t_l)_{D1}(t_4 + \Delta t_s)_{D2} : P_1^2R_1\eta_l T_1\eta_s T_2^2 \\ &(t_4 + \Delta t_s)_{D1}(t_3 + \Delta t_l)_{D2} : P_1^2R_1\eta_l T_1\eta_s R_2^2 \end{aligned} \tag{4.9}$$

However, these expressions are only valid under the assumptions that the two photons are fully distinguishable and no HOM quantum interference takes place at the second

beam splitter. If the photons are fully indistinguishable, the probability of both detectors clicking simultaneously is dependent only on the asymmetry in splitting ratio of the last beam splitter (BS_2). The expression for the correlations at $\Delta\tau = 0$ is again the sum of the four contributions, but contrary to the previous two regimes ($\Delta\tau = \pm 2t_d$, $\Delta\tau = \pm t_d$) here we differentiate between photons being either fully indistinguishable ($A_{0\parallel}$) or fully distinguishable ($A_{0\perp}$):

$$A_{0\parallel} = P_1^2 \left\{ g^{(2)}(0) R_2 T_2 \left(R_1^2 \eta_l^2 + T_1^2 \eta_s^2 \right) + R_1 \eta_l T_1 \eta_s \left(T_2 - R_2 \right)^2 \right\} \tag{4.10}$$

$$A_{0\perp} = P_1^2 \left\{ g^{(2)}(0) R_2 T_2 \left(R_1^2 \eta_l^2 + T_1^2 \eta_s^2 \right) + R_1 \eta_l T_1 \eta_s \left(T_2^2 + R_2^2 \right) \right\} \tag{4.11}$$

4.2.3 HOM visibility and indistinguishability

As stated before, an important use of the Mach-Zehnder interferometer is to measure the single-photon indistinguishability of a single-photon source. This is generally done by linking the indistinguishability M to the Hong-Ou-Mandel interference visibility $\mathcal{V}_{\mathrm{HOM}}$ [61, 64, 66]. However, most of these contributions assume that the interferometer is perfectly balanced in intensity and the beam splitters are exactly 50:50. Here we develop a more general expression. The HOM visibility is defined as a function of the correlations at $\Delta\tau = 0$ for distinguishable ($\perp$) and indistinguishable ($\parallel$) photons normalized to the coincidences for the distinguishable case:

$$\mathcal{V}_{\mathrm{HOM}} = \frac{g_{\perp}^{(2)}(0) - g_{\parallel}^{(2)}(0)}{g_{\perp}^{(2)}(0)} \tag{4.12}$$

The necessary correlations can be calculated from our results above as $g_{\perp}^{(2)}(0) = A_{0\perp}/A_{\pm}$ and $g_{\parallel}^{(2)}(0) = A_{0\parallel}/A_{\pm}$.

Equations 4.10 and 4.11 describe the cases of either fully indistinguishable or fully distinguishable photons. To account for experimental imperfections in wavefunction overlap, we extend this model to arbitrary degrees of distinguishability and replace M by MV_p, where the polarization overlap V_p is controlled experimentally. By linear interpolation we obtain a general expression for the correlations at $\Delta\tau = 0$:

$$A_0 = MV_p A_{0\parallel} + (1 - MV_p) A_{0\perp} \tag{4.13}$$

Experimentally, to measure the HOM visibility Eq. 4.12, we determine the two-photon correlations for both maximum and minimum wavefunction overlap. For minimum overlap, the polarization state in one arm of the interferometer is set orthogonal to that in the other; for maximum overlap, the polarization states in both interferometer arms are identical. To account for imperfections in the polarization alignment, we distinguish between the two cases by defining separate polarization overlaps: $V_{p,\parallel}$ for the parallel configuration, and $V_{p,\perp}$ for the orthogonal one. These are substituted into Equation 4.13 in place of V_p when calculating A_0 for $g_{\parallel}^{(2)}(0)$ and $g_{\perp}^{(2)}(0)$. Usually, the values of $V_{p\parallel}$ and $V_{p\perp}$ are close to 1 and 0, respectively. With this we finally derive a general expression for the indistinguishability M as a function of the HOM visibility and all parameters of the MZI (a step by step derivation of this final expression is given in Appendix 4.6.1):

$$M_{\text{full}} = \frac{\mathcal{V}_{\text{HOM}}\left[T_1\eta_s R_1\eta_l\left(T_2^2+R_2^2\right)+g^{(2)}(0)R_2T_2\left(T_1^2\eta_s^2+R_1^2\eta_l^2\right)\right]}{2T_1\eta_s R_1\eta_l R_2T_2\left[V_{p\parallel}-V_{p\perp}\left(1-\mathcal{V}_{\text{HOM}}\right)\right]} \tag{4.14}$$

Comparison to literature

If we use the assumptions of an ideal interferometer, with balanced transmission ($\eta_s = \eta_l$), perfect beam splitters ($R_1 = T_1 = R_2 = T_2 = 1/2$) and perfect polarization state overlap ($V_{p\parallel} = 1$ and $V_{p\perp} = 0$), Eq. 4.14 reduces to

$$M_{\text{simple}} = \mathcal{V}_{\text{HOM}}\left(1+g^{(2)}(0)\right). \tag{4.15}$$

This is in perfect agreement with results presented in Refs. [61–64,73]. However, our result differs by a factor 2 with the expressions for the indistinguishability used in Refs. [66,74], caused by a difference in the multi-photon part of the derivation (last term of Eq. 4.4). We have analyzed the case and found that the resulting error is small for single-photon sources with high single-photon purity, as is the case case in Refs. [66, 74] - but it still leads to an overestimation of the photon indistinguishability of 1.9%.

4.3 Experiment

We now discuss our experimental setup and procedure.

4.3.1 Experimental setup

Excitation scheme

The quantum dot is excited resonantly using a narrow-linewidth frequency-tunable continuous-wave (CW) laser out of which short pulses are carved using two cascaded electro-optic modulators (EOMs) controlled by custom-made electronics [72] (Fig. 4.5). This enables tunability of both the pulse period and pulse widths at a well-defined center wavelength.

The quantum dot device

The quantum dot itself is a negatively charged self-assembled InGaAs/GaAs dot embedded in a microcavity [66, 75–77]. A 31.8 nm thick tunnel barrier separates the p-i-n junction from the electron reservoir enabling quantum-confined Stark effect tuning of the QD resonance wavelength at around 935 nm [71, 77, 78]. The quantum dot is kept at a temperature around 4 K in a closed-cycle cryostat with optical access. The resonant excitation laser light is focused on the quantum dot by an aspheric lens (Thorlabs A240-B) which is placed inside the cryostat to minimize loss of single-photons. The excitation laser is filtered out using a polarization extinction method (PE and PD in Fig. 4.5) enabling extinction of the order of 10^{-6} [79], and the single-photons are collected in a polarization maintaining (PM) single mode fiber.

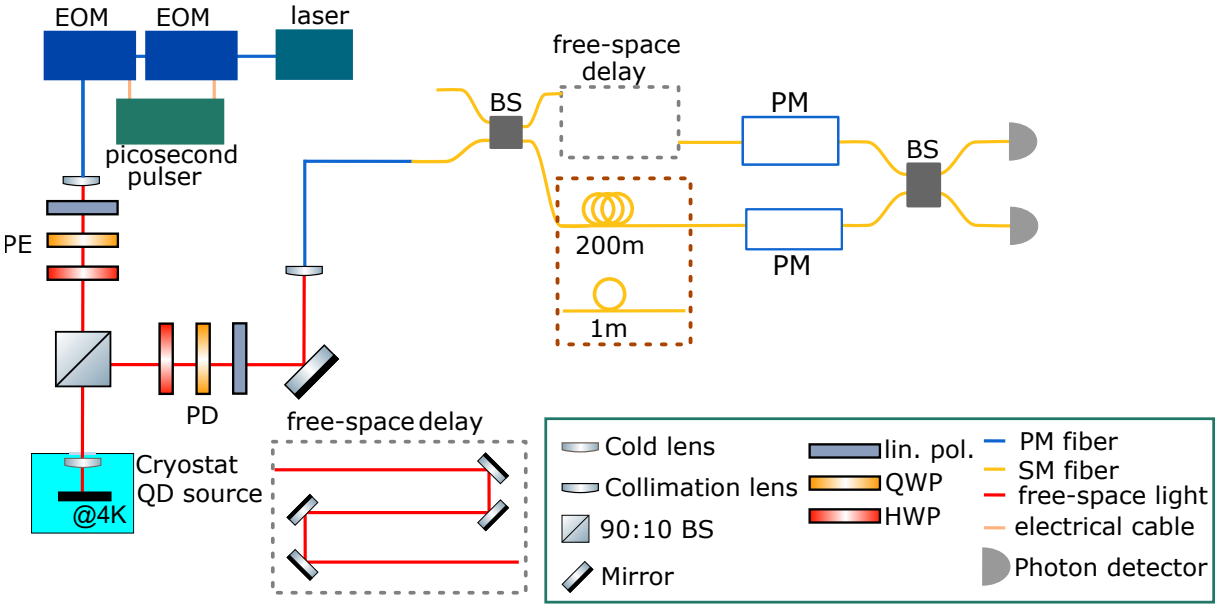


Figure 4.5: Schematic of the experimental setup. Two cascaded electro-optic modulators (EOMs) are used to generate picosecond pulses for excitation of the quantum dot. The polarization state of the excitation laser is optimized in the excitation path (PE) and the excitation laser is filtered out through cross polarization in the detection path (PD). The Mach-Zehnder interferometer consists of two beam splitters (BS) and either has an optical path length difference of 9 ns ($\sim$ 1.8 meters) or 1 µs (200 m). A polarization modulator (PM) in each arm is used to modulate the polarization state overlap V_p

The Mach-Zehnder interferometer

The interferometer shown in Fig. 4.5 consists of two approximate 50:50 fiber-based beam splitters (BS, Thorlabs A240-B for the short delay and OZ Optics FUSED-22 for the long delay). In the lower arm of the interferometer, additional optical fiber of 1 m or 200 m introduces a path delay, which is fine-tuned by the tunable free-space delay in the upper arm. A fiber-based polarization modulator (PM; Polarite III PCD-M02) is placed in both arms of the interferometer to tune the polarization state overlap at the second fiber splitter such that both $g_{\parallel}^{(2)}$ and $g_{\perp}^{(2)}$ can be measured. The photons are detected by two avalanche single-photon detectors (Excelitas SPCM-AQRH-14-FC-ND) and we use a time-tagging card (Cronologic HPTDC, 100 ps resolution) together with custom software to record 2-fold coincidence detection events.

4.3.2 Experimental procedure

The temporal overlap between photons traveling through the two arms of the MZI is optimized by tuning the free-space delay in the upper arm of the interferometer. First we use short laser pulses in combination with low-jitter (40 ps) single-photon detectors and a different correlation card (Becker Hickl SPC-130) for a coarse alignment, and then we fine-tune the temporal alignment by optimizing HOM interference of photons from our single-photon source. For measuring the single-photon purity of the single-photon source with a HBT measurement, we block the free-space delay. For the HOM measurement we tune the polarization state overlap with the polarization modulators; the polarization condition is characterized before and after the experiment, with the use of a polarimeter (Thorlabs PAX1000IR1), to asses polarization drifts.

4.4 Results

The measured two-photon correlations for both the short (9 ns) and long (1 μs) delay in the Mach-Zehnder interferometer are shown in Fig. 4.6, where in panels (a) and (c) the polarization in both arms of the interferometer is set to be the same ($\parallel$), and in (b) and (d) orthogonal ($\perp$). For the short (long) delay experiments we used a laser excitation pulse period of 9 ns (4 ns), a laser pulse width of 58 ps (47 ps), and an integration time of 3 minutes (5 minutes).

In Fig. 4.6 we use the same color scheme as before in Figures 4.1 and 4.3, where red denotes the correlations at $\Delta\tau = 0$, purple the correlations at $\Delta\tau = \pm t_d$ (where $t_d \approx 8.95$ ns for the short delay and $t_d \approx 995.35$ ns for the long delay), and blue corresponds to all other correlations. The values of all relevant correlations are shown in Table 4.1, for which we used a time-bin width of 2 ns. A nonzero background can be observed for all four of the correlation measurements, this is caused by leakage of the excitation laser light due to imperfect cross-polarization filtering and reduced contrast of the excitation laser pulses.

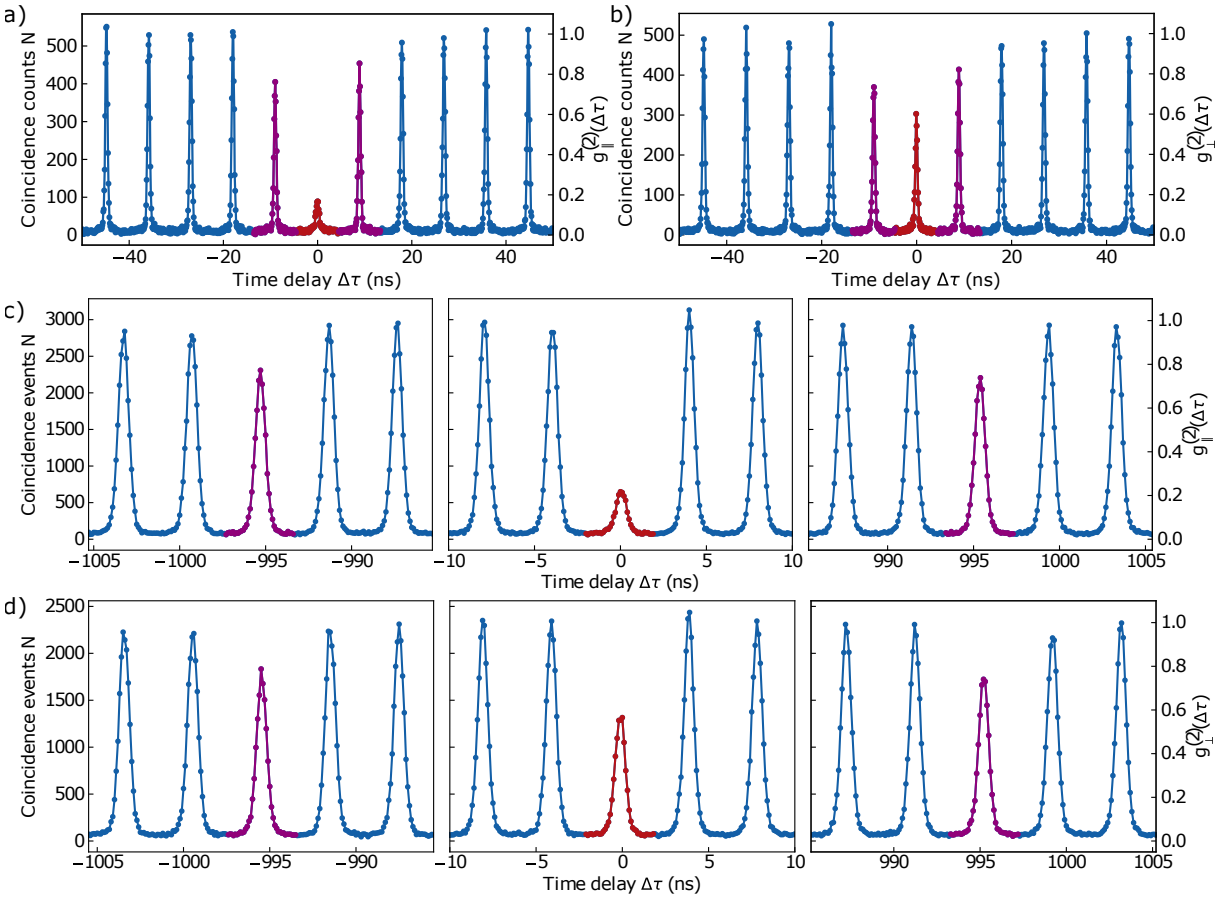


Figure 4.6: Two-photon correlations for both maximized ($\parallel$) and minimized ($\perp$) wavefunction overlap for 9 ns (a & b) and 1 µs (c & d) delay in the MZI.

	short delay (9 ns)			long delay (1 µs)		
	measured		model	measured		model
	$g^{(2)}_{\parallel}$	$g^{(2)}_{\perp}$		$g^{(2)}_{\parallel}$	$g^{(2)}_{\perp}$	
$g^{(2)}_{\parallel}(0)$	0.255±0.009	-	0.245	0.237±0.004	-	0.239
$g^{(2)}_{\perp}(0)$	-	0.608±0.017	0.586	-	0.609±0.007	0.616
$g^{(2)}(+t_d)$	0.824±0.020	0.841±0.022	0.828	0.788±0.008	0.783±0.009	0.803
$g^{(2)}(-t_d)$	0.760±0.019	0.777±0.020	0.763	0.804±0.008	0.799±0.009	0.815

Table 4.1: Comparison between the measured $g^{(2)}$ values for $\Delta\tau = 0$ and $\Delta\tau = \pm t_d$ and the outcome of the model using M_{full}.

From the two-photon correlations we calculate the single-photon indistinguishability M using the method explained in Section 4.2, the results are shown in Table 4.2. We compare the measured HOM interference visibility with the simplified expression assuming an ideal interferometer (Eq. 4.15) and the full expression (Eq. 4.14). From the comparison between $\mathcal{V}_{\text{HOM}}$ with M_{simple} we see that in our case, the purity has a significant impact

	9 ns	1 µs
$\mathcal{V}_{\mathrm{HOM}}$	0.581	0.612
M_{simple}	0.690	0.757
M_{full}	0.834	0.770

Table 4.2: Comparison of the Hong-Ou-Mandel visibility $\mathcal{V}_{\mathrm{HOM}}$ and the extracted indistinguishability comparing the standard simple calculation which is assuming a perfect MZI M_{simple} (Eq. 4.15) with the outcome of the full calculation without assumptions on the experimental parameters M_{full} (Eq. 4.14). All experimental parameters are given in Appendix 4.6.2.

on the estimation of the indistinguishability of the single-photon source. Furthermore, we see that the difference between outcomes of M_{simple} and M_{full} for the longer delay is quite small (0.013), while for the shorter delay the difference is much more significant (0.144). The biggest difference between the two sets of measurements is that for the longer delay the polarization state stability for the duration of the measurement was better with a shift in polarization of 1.4%, while the short-delay experiment had a shift in polarization of 30.3%. Because only the full model takes this polarization shift into account only the M_{full} for 9 ns photon separation is higher than for 1 µs as expected.

Next to the calculation of the indistinguishability, we compare the measured and modeled values of the second-order correlation function measured at $\Delta\tau = 0$ and $\Delta\tau = \pm t_d$ in Table 4.1. As stated before, the modeled $g^{(2)}$ values are calculated by using the appropriate expression for A (Eqs. 4.5, 4.6, 4.10, 4.11) and divide it by the expression for the side-peaks used for normalization $A_{\pm}$ (Eq. 4.3). We see that the model is in very good agreement with the measured data where all model outcomes fall within or are close to the error margin of the measured values. The errors are not taking into account inaccuracies of the measured values of the MZI parameters such as transmission.

Comparing the value of $g^{(2)}(\pm t_d)$ for both interferometers, we find that there is a greater asymmetry for the short delay MZI ($|g^{(2)}(t_d) - g^{(2)}(-t_d)| \approx 0.064$) than for the long delay MZI ($|g^{(2)}(t_d) - g^{(2)}(-t_d)| \approx 0.016$), which is also clearly visible in Fig. 4.6. Interestingly, this height difference is exactly the same for the $\parallel$ and $\perp$ measurements. The most significant contribution is the imbalance in the second beam splitter which is greater in the short delay measurement ($R_2 = 0.54$) than in the long delay measurement ($R_2 = 0.492$). The difference between the reflection and transmission coefficients between the two interferometers is not large ($< 5\%$) but it shows that the $g^{(2)}(\pm t_d)$ correlations are quite sensitive to this imbalance, more than the $g^{(2)}_{\parallel,\perp}(0)$ correlations are.

4.5 Conclusions and outlook

We have examined a single-photon stream in a Mach-Zehnder interferometer (MZI) beyond assessing photon indistinguishability by Hong-Ou-Mandel two-photon correlations. We highlighted that the correlations observed in such setup carry more information than just the overlap of single-photon wave packets, and that experimental imperfections should be taken into account. First, for a perfect interferometer, we explained intuitively the

correlations for a time difference equal to the delay between the interferometer arms $\Delta\tau = \pm t_d$. Then, we developed an analytic model that takes many experimentally relevant parameters into account, explaining the three different classes of correlations: the center correlations at $\Delta\tau = 0$, the correlations corresponding to the interferometer time-delay at $\Delta\tau = \pm t_d$, and all other correlations. We obtained a generalized description of the indistinguishability M as a function of properties that are important for any Mach-Zehnder interferometer experiment. Simplifying the expression for M for an ideal experiment results in the known expression [61–64, 68, 73]. We apply our theory to experimental data obtained with a quantum dot - microcavity single-photon source and a Mach-Zehnder interferometer with both short (9 ns) and a long (1 µs) delays. We observe very good agreement for all correlations. Our clear formulas and model taking experimental imperfections into account might be broadly useful for photonic quantum information research and applications. A similar model could be extended to multi-photon interference in a Sagnac interferometer [71]. This knowledge is essential for error-benchmarking in probabilistic-gate linear cluster state generation schemes [80, 81].

4.6 Appendix

4.6.1 HOM visibility and indistinguishability

Here we show details on the derivation of the final expression for the indistinguishability M_{full} (Eq. 4.14 in the main text). Equation 4.13 in the main text shows that for an arbitrary polarization state overlap the correlation probability at $\Delta\tau = 0$ can be written as:

$$A_0 = MV_pA_{0\parallel} + (1 - MV_p)\, A_{0\perp} \tag{4.16}$$

where V_p is the polarization state overlap of the photons in the different arms of the interferometer and $A_{0\parallel}$ and $A_{0\perp}$ are the correlations at $\Delta\tau = 0$ for fully indistinguishable ($\parallel$) or fully distinguishable ($\perp$) photons:

$$\begin{aligned} A_{0\parallel} =& P_1^2 \left\{ g^{(2)}(0) R_2 T_2 \left(R_1^2\eta_l^2 + T_1^2\eta_s^2 \right) + R_1\eta_l T_1\eta_s \left(T_2 - R_2 \right)^2 \right\} \\ A_{0\perp} =& P_1^2 \left\{ g^{(2)}(0) R_2 T_2 \left(R_1^2\eta_l^2 + T_1^2\eta_s^2 \right) + R_1\eta_l T_1\eta_s \left(T_2^2 + R_2^2 \right) \right\} \end{aligned} \tag{4.17}$$

If we substitute the expressions from Eq. 4.17 into Eq. 4.16 we obtain after simplification

$$A_0 = P_1^2 \left\{ g^{(2)}(0) R_2 T_2 \left(R_1^2\eta_l^2 + T_1^2\eta_s^2 \right) + R_1\eta_l T_1\eta_s \left(T_2^2 + R_2^2 \right) - 2MV_pR_1\eta_l T_1\eta_s R_2 T_2 \right\}. \tag{4.18}$$

The definition of the HOM interferometric visibility is

$$\mathcal{V}_{\text{HOM}} = \frac{g_\perp^{(2)}(0) - g_\parallel^{(2)}(0)}{g_\perp^{(2)}(0)}, \tag{4.19}$$

where the necessary correlations can be calculated from our analysis as $g_\perp^{(2)}(0) = A_0(V_{p\perp})/A_\pm$ and $g_\parallel^{(2)}(0) = A_0(V_{p\parallel})/A_\pm$. Therein, for example, $A_0(V_{p\perp})$ is the expression given in 4.18 for the measured polarization state overlap when polarization states in the two arms of the interferometer were set to be orthogonal. Inserting these definitions into the definition of $\mathcal{V}_{\text{HOM}}$ results in

$$\mathcal{V}_{\text{HOM}} = \frac{2MR_1\eta_l T_1\eta_s R_2 T_2 \left(V_{p\parallel} - V_{p\perp} \right)}{g^{(2)}(0) R_2 T_2 \left(R_1^2\eta_l^2 + T_1^2\eta_s^2 \right) + R_1\eta_l T_1\eta_s \left(T_2^2 + R_2^2 \right) - 2MV_{p\perp}R_1\eta_l T_1\eta_s R_2 T_2}. \tag{4.20}$$

The final step is to rewrite Equation 4.20 to obtain the expression for indistinguishability

$$M_{\text{full}} = \frac{\mathcal{V}_{\text{HOM}} \left[T_1\eta_s R_1\eta_l \left(T_2^2 + R_2^2 \right) + g^{(2)}(0) R_2 T_2 \left(T_1^2\eta_s^2 + R_1^2\eta_l^2 \right) \right]}{2T_1\eta_s R_1\eta_l R_2 T_2 \left[V_{p\parallel} - V_{p\perp} \left(1 - \mathcal{V}_{\text{HOM}} \right) \right]}. \tag{4.21}$$

4.6.2 Experimental parameters

Table 4.3 shows all required experimental parameters to calculate the indistinguishability of our single-photon source using the full model M_{full}, as well as the model outcomes for the two photon correlations at $\Delta\tau = 0$ and $\Delta\tau = \pm t_d$ which are shown in Table 4.1 in the main text.

	short delay (9 ns)	long delay (1 µs)
$g^{(2)}(0)$	0.187±0.015	0.237±0.007
$V_{p\parallel}$	0.846	0.98552
$V_{p\perp}$	0.231	0.00584
R_1	0.47	0.484
T_1	0.53	0.516
η_l	0.627	0.657
η_s	0.602	0.628
R_2	0.54	0.492
T_2	0.46	0.508

Table 4.3: Overview of experimental parameters needed to calculate M_{full} for both the short delay and long delay MZI.

5 Slow temporal demultiplexing of single photons and the normalization of two-photon correlations

To generate temporally coincident photons from a solitary single-photon source, individual photons must be extracted from a continuous stream and temporally synchronized. This process is essential for characterizing photon indistinguishability via the Hong-Ou-Mandel effect and is also relevant for applications in quantum photonics. In this work, we investigate deterministic, switch-based routing of single photons emitted by a quantum dot cavity-QED source. We focus on the regime in which the photon generation rate significantly exceeds the demultiplexing time scale and analyze the resulting long-timescale photon correlation patterns. Our measurements reveal triangular oscillations in the coincidence counts, which complicate the normalization of the second-order correlation function.

5.1 Introduction

Many quantum network and computing applications require more than one single photon, and often those photons must be mutually indistinguishable and propagate at well-defined times in individual optical modes. Traditionally, spontaneous parametric downconversion (SPDC) is used to produce heralded single photons and photon pairs [82, 83]. Since the SPDC process is inherently probabilistic this poses limits on the rate or single-photon brightness and single-photon purity of the obtained photon states [84, 85]. For the generation of *true* single photons a quantum nonlinearity is required for instance enabled by semiconductor quantum dots [84]. Recent progress with quantum-dot micro-cavity based devices has enabled high-purity sources of single photons with high brightness at excellent purity outperforming SPDC sources [60, 66, 67, 72, 75, 85, 86]. Those sources, however, produce a stream of photons in a single spatial mode, which therefore requires temporal demultiplexing into multiple spatial modes [87, 88] and their synchronization. If the single-photon source brightness is near-unity and the demultiplexing mechanism is low-loss, such demultiplexed quantum dot sources could power future optical quantum computers [57], but they also enable quantum network applications involving more than one photon [12, 17, 89]. Obviously, probabilistic beam splitter-based demultiplexing is not an option as it leads to a low success rate. Since the single-photon indistinguishability degrades with the time delay between photon production times by spectral diffusion and other decoherence mechanisms [66], fast switching (≤ 1 µs) is essential, while maintaining low-loss operation.

There are several approaches to photon switching or routing [90] that can be used for demultiplexing: Mechanical MEMS-based switching which are rather slow [91], and switches based on electro-optical modulation (EOM, [92]) either of the photon polarization or the phase, the latter in combination with Mach-Zehnder interferometers (MZI) or micro ring resonators [93]. Due to unavoidable insertion loss in integrated optics, often, free-space EOMs are used which however require high electrical drive powers and special EOM coatings to provide low-loss and high-fidelity switching [94]. Commercially, low-loss integrated-optics and fiber-coupled optical switches that operate at a suitable wavelength for InGaAs quantum dots, around 930 nm, are rather rare - in addition, since quantum dot photons are spectrally rather wide, large-bandwidth (nm range) operation is needed. Known approaches are custom integrated-optics devices [87], free-space electro-optic polarization modulation (also by the Pockels effect) and separation [88, 95–99], and integrated-optics devices [57].

We investigate an optical switch based on an EOM embedded within an MZI, with a switching time of 1 µs and an insertion loss of 0.25 dB. We focus on its application to the temporal demultiplexing of a quantum dot single-photon stream in a regime where the photon generation rate (~100 MHz) significantly exceeds the switching frequency (1 MHz). We analyze the performance of the demultiplexed photons in terms of their purity and indistinguishability, as determined through Hanbury Brown and Twiss (HBT) and Hong-Ou-Mandel (HOM) measurements. Due to the presence of triangular oscillations in the second-order correlation function, a more rigorous normalization procedure is required than is commonly used in conventional MZI-based experiments.

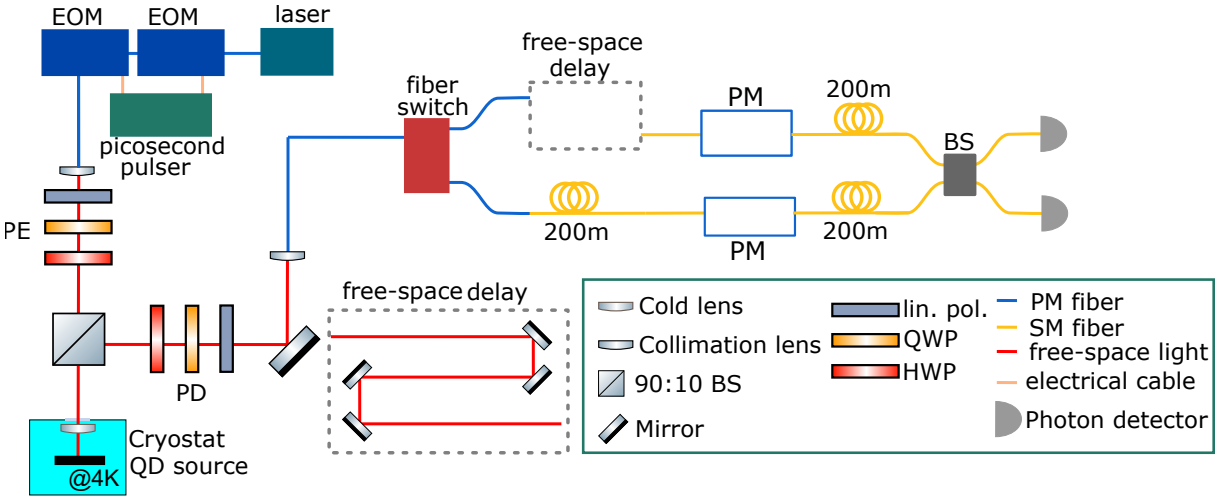


Figure 5.1: Schematic of the experimental setup. Two cascaded electro-optic modulators (EOMs) are used to generate picosecond optical pulses that excite the quantum dot source (PE and PD are polarization controllers in the excitation and detection paths). Photons are split by the fiber switch, synchronized by the 200 m fiber delay and a free-space delay line before being polarization controlled by the in-fiber polarization modulators (PM). The correlation measurements are done using a fiber-based beam splitter (BS) with two avalanche single-photon detectors.

5.2 Experimental setup

The QD is excited using short pulses [72] produced out of a narrow-linewidth frequency-tunable continuous-wave (CW) laser light using two cascaded electro-optic modulators (EOMs) controlled by custom-made electronics (see Fig. 5.1). These pulses have tunable widths and pulse period at a well-defined center wavelength. We use a single negatively charged self-assembled InGaAs/GaAs quantum dot (QD) at 4 K embedded in a micro-cavity as a single-photon source [66, 75–77]. In the device, a 31.8 nm thick tunnel barrier separates the QDs from the electron reservoir enabling quantum-confined Stark effect tuning of the QD resonance wavelength at around 935 nm [71, 77, 78]. The resonant excitation laser is filtered out using a cross-polarization method, enabling around 10^{-6} extinction [79], and the single photons are collected in a polarization maintaining (PM) single mode fiber. We use a laser power of approximately 3 nW measured in front of the window of the cryostat window.

In order to split the single-photon stream we use an optical fiber switch (Agiltron NPNS) as shown in Fig. 5.1. Because this device is relatively slow with a switching time of 1 µs, a 200 m long optical fiber is used to synchronize the sliced photon streams. We use a free-space delay line in addition to the 200 m long fiber to obtain an optical delay of exactly 1 µs, the switching time. This allows us to fine-tune the temporal wavefunction overlap of the photons at the final beam splitter.

To control the overlap of the photons in polarization space, we use two piezoelectric fiber-based polarization modulators (Polarite III PCD-M02) in each of the arms with which any arbitrary polarization state can be prepared. On each side of the interferometer arm there is an additional 200 m long 780HP single-mode fiber.

The two arms are recombined in a fiber-based beam splitter (Thorlabs TW930R5A2) and photons are detected using two single-photon avalanche detectors (SPADs, Excelitas SPCM-AQRH-14-FC-ND). We use a time-tagging card (Cronologic HPTDC, 100 ps resolution) together with custom software to obtain the two-photon correlations.

We align the temporal overlap by carefully tuning the free-space delay line. First we use short (50 ps) laser pulses in combination with faster detectors (idQuantique ID100-MMF50 SPADs, 50 ps jitter) and a different correlation card (Becker&Hickl SPC-130; start-stop correlations) for a coarse alignment, before we fine-tune the temporal overlap by optimizing HOM interference of single photons. After alignment we measure the purity of the single photons in the system by performing a Hanbury Brown and Twiss (HBT) experiment. For this, we block on arm within the free-space delay line to make sure that no two-photon HOM interference can take place. For the HOM measurement, we use both arms and tune the polarization state overlap with the polarization modulators. To characterize the polarization states in the two arms, we use continuous-wave laser light of the same frequency as used for QD excitation and measure the Stokes parameters with the use of a polarimeter (Thorlabs PAX1000IR1). This is done only before and after the correlation experiments to monitor drifts in the polarization state overlap.

5.3 Results

5.3.1 Short-time photon correlations

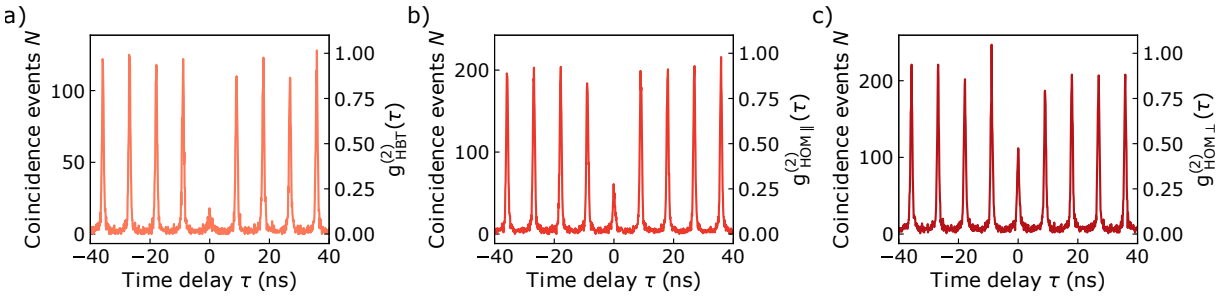


Figure 5.2: Purity and indistinguishability. With the Hanbury Brown and Twiss experiment we measure the photon purity (a), and by two-photon Hong-Ou-Mandel interference we determine the single-photon indistinguishability by comparing parallel (b) and perpendicular (c) polarization of the photons. In each figure, the left y-axis shows the raw coincidence events measured in the 5 minutes-long measurements, and the right axis shows the corresponding normalized second-order correlation function.

In Fig. 5.2 we show photon correlations measured in the HBT and HOM configuration, the latter for parallel (HOM$\parallel$) and orthogonal (HOM$\perp$) polarization of the interfering photons. The cascaded EOM pulser was set to a pulse period τ_l of 9 ns and a pulse width of 58 ps. Correlations were recorded over a time span of 5 minutes, and from this the photon coincidences were calculated up to a time delay of 200 ns, where the zero delay point was offset by 59 ns.

In order to obtain reliable values of the second order correlation function at zero-time delay $\left(g^{(2)}(0)\right)$, we determine coincidences in time-bins centered around the peaks. We

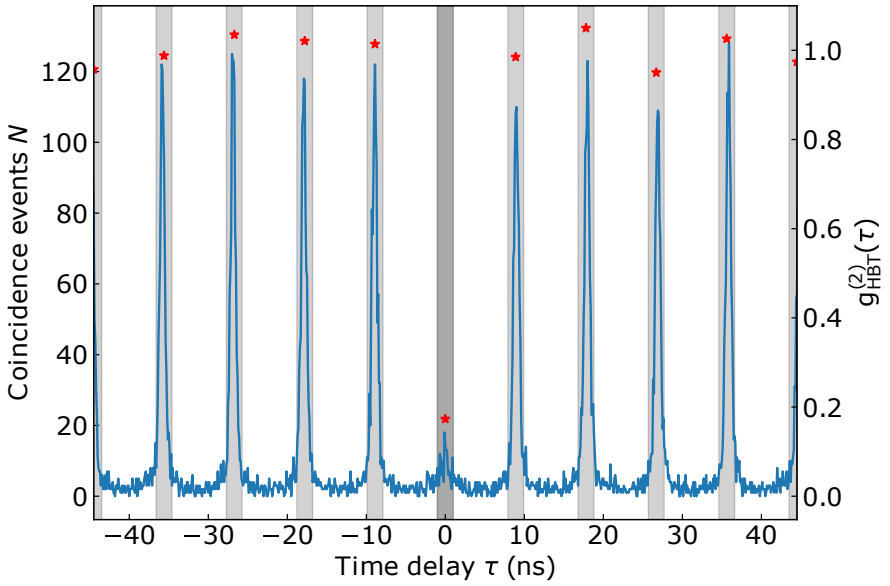


Figure 5.3: Correlation binning. To illustrate how we evaluate photon correlations, we show the HBT measurement (Fig. 5.2(a)). The gray areas show the temporal windows used to calculate the coincidence events, N_0 for the central peak at $\tau = 0$, and N_{side} for the five peaks on the left and right. The red symbols show the binned coincidence events and $g^{(2)}$ values after normalization.

determine the coincidences N_0 in the central time-bin at $\tau = 0$ as well as the averaged coincidences over the ten surrounding time-bins (five on each side of $\tau = 0$) $\bar{N}_{\text{side}}$. This allows us to normalize the coincidences and obtain $g^{(2)}(0) = N_0/\bar{N}_{\text{side}}$. An example of this normalization procedure is shown in Fig. 5.3 where the gray shaded areas indicate the 2 ns wide time bins, and the red stars the calculated $g^{(2)}$ values for each of the time bins. Table 5.1 shows the numeric results. With these numeric results we can also give a value of both the HOM interferometric visibility (Eq. 5.1) and the indistinguishability (Eq. 5.2) of the single-photon source [62, 100], resulting in $\mathcal{V}_{\text{HOM}} = 0.456 \pm 0.028$ and $M_{\text{simple}} = 0.535 \pm 0.054$.

$$\mathcal{V}_{\text{HOM}} = \frac{g^{(2)}_{\text{HOM}\perp}(0) - g^{(2)}_{\text{HOM}\parallel}(0)}{g^{(2)}_{\text{HOM}\perp}(0)} \tag{5.1}$$

$$M_{\text{simple}} = \mathcal{V}_{\text{HOM}} \left(1 - g^{(2)}_{\text{HBT}}(0)\right) \tag{5.2}$$

Equation 5.2 is the simplified version assuming a perfect interferometer. In the previous chapter of this thesis we have shown this not to be always true and we have developed an extended model including experimental imperfections resulting in equation 5.3 below. The description that is derived for a Mach-Zehnder interferometer also applies to the temporal demultiplexing system here, since the switching time is significantly larger than the pulse period of the quantum dot excitation laser. The treatment of R_1 and T_1, the reflection and transmission coefficients of what in the MZI system would be the first beam splitter, is slightly different. For the optical switch, these coefficients correspond

	N_0	$\bar{N}_{side}$	$g^{(2)}(0)$
HBT	174±13	1004±32	0.173±0.014
HOM ∥	573±24	1738±42	0.330±0.016
HOM ⊥	1097±33	1807.3±46	0.607±0.023

Table 5.1: Raw coincidences and second-order correlation function values with corresponding statistical errors, of the measured data shown in Fig. 5.2. N_0 are the counts in the central time-bin, $\bar{N}_{side}$ the averaged counts of the 10 nearest bins (five on each side of $\tau = 0$). $g^{(2)}(0)$ is obtained after normalization.

to the transmissions towards either output (T_1 is towards the top output in Fig. 5.1), and therefore it no longer holds that $R_1 + T_1 = 1$. Coefficients R_2 and T_2 still describe the reflection and transmission coefficients of the final beam splitter (BS in Fig. 5.1). η_s and η_l are the transmissions through the arms of the interferometer and $V_{p\|}$ and $V_{p\perp}$ are the average polarization state overlap measured for the HOM∥ and HOM⊥ correlation measurements. The values of all experimental parameters are given in Appendix 5.5.1 and we obtain an indistinguishability $M_{\text{full}} = 0.545$. Since this is very close to M_{simple} and the difference between $\mathcal{V}_{\text{HOM}}$ and M_{simple} is larger, we can conclude that the purity of the single-photon source is more influencing the indistinguishability than the experimental imperfections.

$$M_{\text{full}} = \frac{\mathcal{V}_{\text{HOM}}\left[T_1\eta_s R_1\eta_l\left(T_2^2+R_2^2\right)+g^{(2)}_{\text{HBT}}(0)R_2T_2\left(T_1^2\eta_s^2+R_1^2\eta_l^2\right)\right]}{2T_1\eta_s R_1\eta_l R_2T_2\left[V_{p\|}-V_{p\perp}\left(1-\mathcal{V}_{\text{HOM}}\right)\right]} \tag{5.3}$$

5

5.3.2 Long-time photon correlations

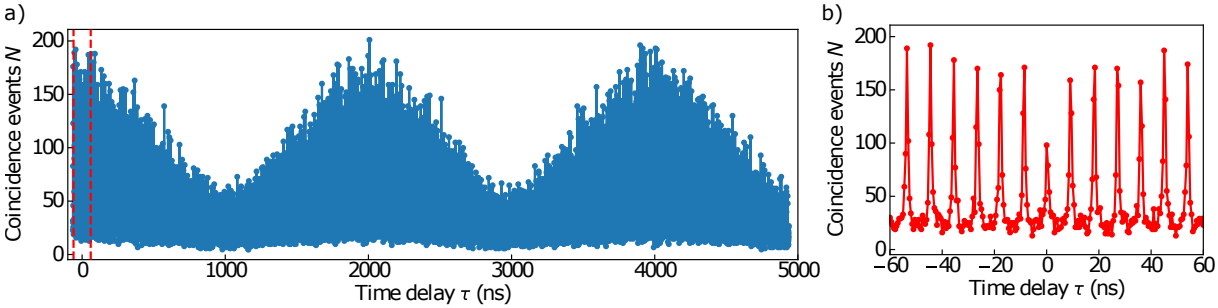


Figure 5.4: Long-time HOM correlations for the switch experiment with a switching time of 1 µs and synchronization. Coincidences are calculated for a time delay of up to 5 µs (a); panel (b) shows a magnification of the region in (a) indicated by dashed lines.

Because the optical switching is much slower than the excitation of the quantum dot, we need to look at a longer time window to see the effect of the switch on the HOM photon correlations. The result is shown in Fig. 5.4(a), which shows correlations with a detection

delay of up to 5 µs with undetermined polarization state overlap. This long time delay is possible by the time-tagging approach and our custom analysis software. The reduced peak at zero time delay appears to be absent, but this is only due to the enormous amount of data, as the correlations measured at zero time delay are clearly visible in the magnified view in Fig. 5.4(b). Furthermore, we observe triangular oscillations of the coincidence peak heights, and to a lesser degree also of the background coincidences between the peaks.

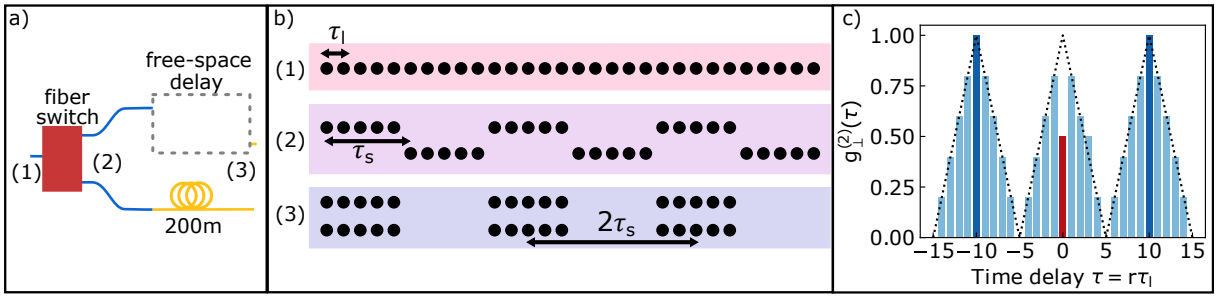


Figure 5.5: Illustration of temporal demultiplexing. We assume that the demultiplexing occurs in bunches of five photons, i.e., the switching time τ_s is five times larger than the time between two consecutive photons τ_l. Schematic representation of the demultiplexing part of the setup (a). Panel (b) shows schematically the single-photon streams before the switch (1), after the switch but before the temporal delay (2) and after the temporal delay (3). The simulated photon correlations assume triangular shape (c), where the dotted lines emphasize the shape of the triangular oscillations that arises.

In order to get a deeper understanding, we now develop a simple model of the temporal demultiplexing experiment which is illustrated in Fig. 5.5(a). We assume the switch to be slow meaning that the switching time τ_s is longer than the time between two consecutive photons in the single-photon stream (or pulse period) τ_l; and for this particular example we assume $\tau_s = 5\tau_l$. Before the switch [(1) in Fig. 5.5(b)] there is a single long stream of photons, and the switch outputs are then routed to the two paths in bunches of five (2). The temporal delay then synchronizes both photon streams (3). This leaves empty time bins, in this example five, followed by five occupied time bins in both streams. This means that during one period and for a time delay $\pm\tau_s$ there is no combination of photons that can result in a coincidence event, while for a time delay of $\pm 2\tau_s$, there are five possibilities, with linear interpolation in between. Hence, the second order correlation function assumes a triangular shape as shown in Fig. 5.5(c). In general, ignoring HOM interference at $\tau = 0$, we obtain zero coincidence events at odd multiples of the switching time, and maximal correlations at even multiples of the switching time. The slope of the resulting triangular oscillations depends on τ_l/τ_s, the ratio between the time delay between two consecutive photons and the switching time. If τ_s is only slightly larger than τ_l, as discussed in this particular example where $\tau_s = 5\tau_l$, the correlations at time delay $\pm\tau_l$ deviate strongly from the maximum correlations (by 20% in Fig. 5.5(c)). If one would use the "standard" method of normalization described earlier it would result in a gross overestimation of $g^{(2)}(0)$ and consequently in wrong purity and indistinguishability values. Therefore, the normalization of experimental data needs to be done carefully, and in principle, only the correlations at even multiples of the switching time should be used.

If, however, like in our case where the switch is much slower than the time between two consecutive photons ($\tau_s \gg \tau_l$), using correlations for normalization around $\tau = 0$ leads to relatively small error, due to slope being shallow in this case.

For instance, in our long-time correlation experiment with $\tau_s = 1$ µs and $\tau_l = 9$ ns, there are approximately 111 peaks underneath one half of the triangular shape, and for normalization we have used the first five side-peaks as shown in Fig. 5.5(c). The difference in $g^{(2)}$ value between two consecutive peaks is theoretically around ≈ 0.009, which results in an averaged peak height of 0.973 instead of 1.0, adding 3 % error to $g^{(2)}$. To confirm this claim we tested both the method displayed in Fig. 5.3, henceforth named the "nearby normalization", and the method where only correlations corresponding to a multiple of the switching time τ_s are used for normalization, to which we will refer to as the "exact normalization", on the long time delay data from Fig. 5.4. For both methods time bins of 3 ns were used. The values of the coincidences in the central time bin N_0, the average coincidences in the time bins used for normalization $\bar{N}_{side}$ and the resulting correlations at zero time delay $g^{(2)}(0)$ are shown in table 5.2. The value of N_0 is naturally independent of the method, since the method only affects which surrounding bins are used for the normalization, hence only affecting $\bar{N}_{side}$. The resulting $g^{(2)}(0)$ extracted with the exact normalization is smaller by 0.03 compared to the $g^{(2)}(0)$ calculated with the nearby normalization. This corresponds to a difference of 4 % which is comparable to the expected error of 3 %.

Normalization:	nearby	exact
N_0	383±20	
$\bar{N}_{side}$	542±23	566±24
$g^{(2)}(0)$	0.71±0.05	0.68±0.05

Table 5.2: Model comparison. Coincidences in the central time bin N_0, the average coincidences in the time bins used for normalization $\bar{N}_{side}$ and the resulting correlations at zero time delay $g^{(2)}(0)$ comparing the "nearby normalization" and "exact normalization" method applied to the long time delay coincidences shown in Fig. 5.4.

Finally, we observe in Fig. 5.4(a) that the offset also oscillates synchronously with the peak height. The offset is more clearly visualized in Fig. 5.4(b) and is caused by a multi-photon component mostly caused by imperfect extinction of the excitation laser. These unwanted photons are also routed to the two paths and the same arguments hold as explained for the single photons, therefore the offset oscillation is expected. The apparent rounding of the triangular oscillations is mostly likely caused by the shot noise in the measurement.

5.4 Conclusions and outlook

We have investigated how temporal demultiplexing influences the second order correlation function and found that normalization has to be done carefully. In a Hong-Ou-Mandel experiment with an optical switch with a switching time τ_s =1 µs that is much larger than the pulse period of the excitation laser τ_l = 9 ns, we have measured two-photon correlations over a period of approximately 5 µs. The correlations show triangular oscillations, which are well explained by a simple model. We find that even in the case of $\tau_s \gg \tau_l$, the normalization error for $g^{(2)}(0)$ can be on the order of a few percent but can be mitigated easily if the oscillations are taken into account.

5.5 Appendix

5.5.1 Experimental parameters

Table 5.3 shows an overview of all required experimental parameters to calculate the indistinguishability M taking account of all imperfections in the interferometer. Unlike a standard MZI system here R_1 and T_1 are the transmission coefficients of the optical fiber switch when either 0 V or 1.4 V is applied and therefore do not add up to 1.

	Temporal demultiplexer
$g^{(2)}(0)$	0.173±0.014
$g^{(2)}_{\parallel}(0)$	0.330±0.016
$g^{(2)}_{\perp}(0)$	0.607±0.023
$\mathcal{V}_{\mathrm{HOM}}$	0.456±0.028
$V_{p\parallel}$	0.9971
$V_{p\perp}$	0.0019
R_1	0.60
T_1	0.71
η_l	0.70
η_s	0.67
R_2	0.54
T_2	0.46

Table 5.3: Experimental parameters.

6 Towards experimental demonstration of quantum position verification using single photons

The geographical position can be a good credential for authentication of a party. This is the basis of position-based cryptography – but classically this cannot be done securely without physical exchange of a private key. Recently it has been shown that by combining quantum mechanics with the speed-of-light limit of special relativity, this might be possible: quantum position verification. Here we demonstrate experimentally a protocol that uses two-photon Hong-Ou-Mandel interference at a beam splitter, which, in combination with two additional beam splitters and four detectors is rendering the protocol resilient to loss. With this, we are able to show first results towards an experimental demonstration of quantum position verification.

This chapter has been published: Kanneworff, K., Poortvliet, M., Bouwmeester, D., Allerstorfer, R., Lunel, P. V., Speelman, F., Buhrman, H., Steindl, P. & Löffler, W. *Towards Experimental Demonstration of Quantum Position Verification Using Single Photons.* Quantum Sci. Technol. **10**, 045004 (2025) [89].

6.1 Introduction

Since the geographical location is often a good credential of a party in communications, verification thereof could add a useful layer to communication security – this is the case, for instance, with data centers, banks, government buildings, a lab in a quantum network, or even a satellite. Classically, position verification is only possible securely by prior physical exchange of keys [1]. In quantum mechanics, mainly thanks to the no-cloning theorem, this can be avoided [2–4,101]. The general scheme of quantum position verification (QPV) is shown in Fig. 6.1: Two verifiers V_0 and V_1 share a private communication channel and aim to confirm the location of a third party, the prover P. The verifiers send classical and quantum information, the prover performs a task and returns classical (and possibly quantum) information. The verifiers use this information and the timing and conclude if the prover was at the claimed position or not. This scheme is one-dimensional but can be extended to higher dimensions [10].

However, it quickly was found that attackers with shared entanglement and exploiting quantum teleportation can break quantum position verification protocols, after first attempts [2,6,7] a general attack was found [15]. This finding has stimulated broad research into the topic [8, 12, 17, 18, 20, 21, 25, 27, 30–35, 102], and it was found that by including classical-information cryptographic tasks, QPV protocols can be made secure for all practical purposes such that attackers require a very large amount of shared entanglement that does only depend on the amount of classical information used in the QPV protocol [22,23].

In real-world QPV, the quantum information is sent by photons, and two major loopholes emerge from this: First, photons are susceptible to loss during transmission, which opens up a generic attack strategy since the adversaries can claim loss if their measurements have been performed in the wrong basis, for instance. Therefore, fully loss-tolerant protocols are required [17, 26, 103], the first having been developed in Refs. [8, 12]. We will investigate here a variation of those protocols, the SWAP protocol developed and analyzed by some of us [18] where two-photon interference makes loss-based attacks detectable. The second major loophole appears if we transport the photons through fiber networks, where the speed of light c is reduced compared to free space, giving attackers using free-space communications an advantage. This slow quantum information loophole we do not address here, but we mention that recently, advanced protocols including a commitment step have been developed [19] that could mitigate this issue in future.

In this chapter, we report our progress towards an experimental demonstration of QPV. We use single photons from a demultiplexed quantum dot – microcavity single-photon source, send them to the two verifiers, encode suitable qubits in the photons and send them to the prover. The prover performs the SWAP test using Hong-Ou-Mandel two-photon interference and measures the result in a loss-tolerant way with 4 single-photon detectors. We analyze the results critically by comparing photon correlations to protocol simulations. Those results show that we currently cannot claim fully secure QPV, and we find that imperfections in our single-photon source are responsible. Finally, we compare our results to a simulated outcome based on our experimental conditions but using the properties of a higher-quality state-of-the-art single-photon source, this suggests that secure QPV with a quantum-dot single-photon source is within reach.

6.2 Protocol

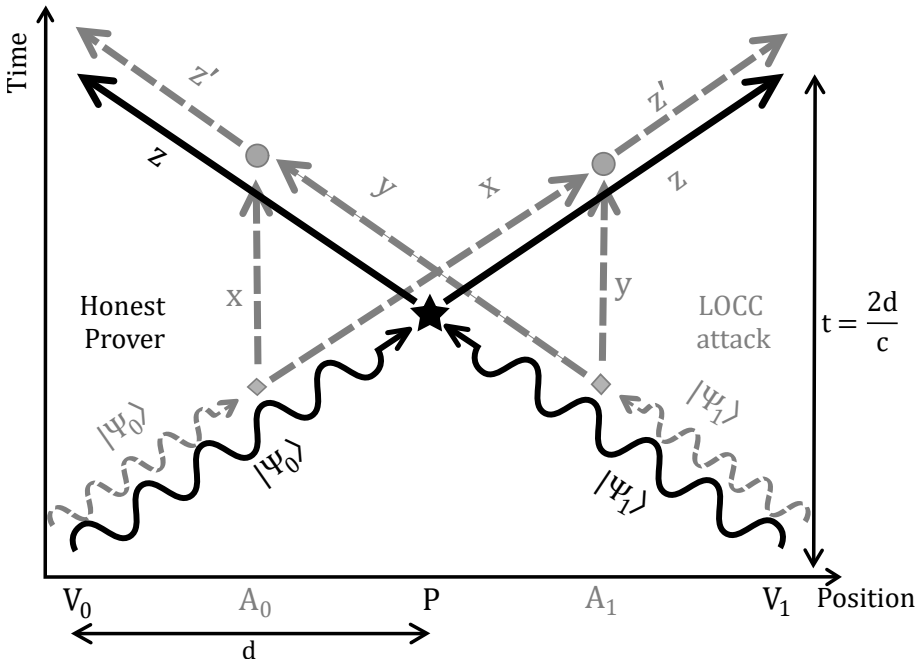


Figure 6.1: Space-time diagram of a one-dimensional QPV protocol showing the prover (P) centered at distance d between two verifiers (V_0 and V_1, solid black) where curly (straight) lines indicate quantum (classical) information exchange. Dashed grey lines show a potential form of attack by two adversaries (A_0 and A_1) positioned around the supposed location of the prover that try to mimic the honest prover responses and are restricted to local operations and classical communication (LOCC). Symbols are explained in the text.

Photon loss is one of the most important limiting factors for any experimental realization of quantum position verification. Most of the proposed QPV protocols are partially loss tolerant meaning that they can only tolerate loss up to a certain fraction such as 50%. However, any loss limit renders a real-world implementation very challenging due to the exponential loss with distance given by the Lambert-Beer law, and limited photon production and detection probability. The first ideas about a fully loss-tolerant QPV protocol were proposed by Qi and Siopsis [8] and a first experimental proposal for such a protocol was developed by Lim et al. [12]. In this protocol, in each round, the verifiers send to the prover either parallel (equal) or orthogonal photonic qubits in a randomly chosen basis. At the prover, the photons interfere at a beam splitter where the Hong-Ou-Mandel effect [37] leads to a different output statistics depending on whether the photons were parallel or orthogonal. This allows the prover to test for qubit equality in a basis-independent way and avoids public communication of the basis which would open a loss-based attack [12]: Adversaries can measure the qubit(s) in a particular basis, if this basis choice turns out to be wrong, they can claim loss. We use here an adaptation of the Lim protocol by Allerstorfer et al. [18], the SWAP protocol. This allows use of all 3 mutually unbiased qubit bases (we, however, show here one basis only), which improves the resilience against noise.

The SWAP protocol entails, see Fig. 6.1:

1. **Preparation:** Verifiers V_0 and V_1 share via their private channel a uniformly drawn random sequence of basis choices and qubit states (parallel or orthogonal), e.g. $|\Psi_0\rangle$ and $|\Psi_1\rangle$. Encoded in the polarization of single photons, these qubits are sent to the prover such that they arrive simultaneously.

2. **Measurement $\star$:** The prover performs the quantum measurement based on two-photon Hong-Ou-Mandel (HOM) quantum interference, we use two additional beam splitters (BSs) and 4 detectors that allows to discriminate HOM photon bunching from loss as explained below. The prover returns a classical response $z = 0$ if they suspect that $|\Psi_0\rangle \parallel |\Psi_1\rangle$, $z = 1$ for $|\Psi_0\rangle \perp |\Psi_1\rangle$, and $z = \oslash$ if the measurement is not conclusive.

3. **Round check:** After each response of the prover, the verifiers review if the received response z is the same for both verifiers and if the response arrived within the set time constraint. If either check fails, the verifiers abort the protocol.

4. **Verification:** After n rounds of steps $1 \ldots 3$, the verifiers check if the distributions of answers returned by the prover $z = \{0, 1, \varnothing\}$ follow the expected distribution within a certain error margin.

6.3 Experiment

6.3.1 The single-photon source

Essential for our experiment shown in Fig. 6.2 is the source of single photons. Although single photons can be produced relatively easily using spontaneous parametric downconversion (SPDC, see e.g. Ref. for a comparison), we choose here to use a source based on quantum dots. We use a single negatively charged self-assembled InGaAs/GaAs quantum dot (QD) embedded in an optical microcavity [66, 75–77]. The QD is embedded in a p-i-n junction separated by a 31.8 nm thick tunnel barrier from the electron reservoir to enable tuning of the QD resonance wavelength at around 935 nm by the quantum-confined Stark effect, for details see Refs. [71, 77, 78]. We drive the QD resonantly with short optical pulses carved out of narrow-linewidth frequency-tunable continuous-wave laser light by using an electro-optic modulator (EOM) controlled by custom-made electronics [72]. This enables production of laser pulses with tunable pulse width of around 100 ps and pulse period (9 ns) at a well-defined center wavelength. These parameters provide a good trade-off between single-photon brightness and quality of the single photons [72]. The single photons are separated from the laser light using a cross-polarization technique enabling laser extinction on the order of 10^{-6} [79] and collected in a polarization-maintaining (PM) single-mode fiber, resulting in an in-fiber single-photon brightness or generation rate of around 3 % .

6.3.2 QPV setup

The overall scheme of the QPV experiment is shown in Fig. 6.2. For the present implementation of the SWAP protocol, we demultiplex and distribute consecutive single

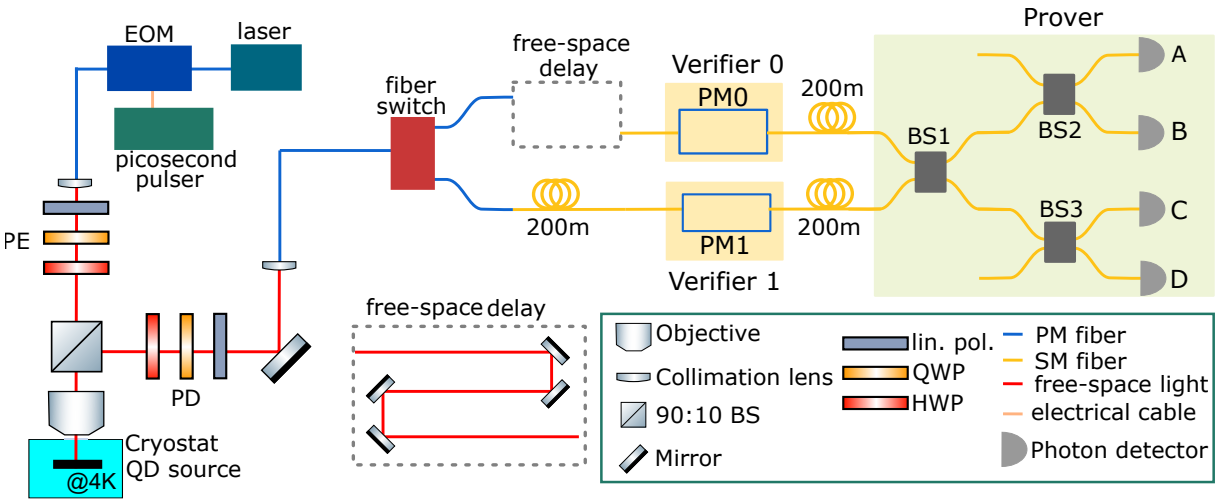


Figure 6.2: Schematic of the experimental setup. The electro-optic modulator (EOM) is used to generate the picosecond pulses, PE and PD are the polarization control elements of the excitation and detection paths, PM0 and PM1 are the polarization modulators of the verifiers, and BS1..3 are 50:50 fiber-based beam splitters, where HOM interference for the SWAP test happens at BS1, and BS2 and BS3 split the outputs of BS1 to two detectors each, while the unused input ports of BS2 (top) and BS3 (bottom) are closed.

photons from the quantum dot source to both verifiers. For this, we first temporally demultiplex photons using a fiber switch (Agiltron NPNS, 500 kHz switching frequency). The time delay of the demultiplexer setup is adjusted to the switching frequency to around 1 µs to synchronize the photons, and an additional free-space delay is used to fine-tune the temporal profile of the single photons to maximally overlap at the first beam splitter BS1 of the prover part of the setup. In a real-world application, one would of course use faster switches based on EOMs and synchronize them to the single photons, but those were not available to us for our operating wavelength. To simulate the distance between the verifiers and the prover, 200 m of single-mode (SM) optical fiber cable (780HP) is used. The overall transmission of the setup is between 7.2% and 12.4%, details are given in Appendix 6.7.1. We do not implement the classical channel for returning the prover answers to the verifiers, this can be done by standard radio-frequency techniques.

Verifiers

Both verifiers encode their qubits into the polarization state of the photons using piezoelectric fiber-based polarization modulators (PM0 and PM1, Polarite III PCD-M02), with which arbitrary polarization states can be prepared.

Calibration

All fibers behind the fiber switch are nonpolarization-maintaining SM fibers, and all induce polarization rotations. We use a fiber coupled polarimeter (Thorlabs PAX1000IR1/M) to calibrate the necessary polarization rotations such that polarization qubits from both verifiers experience during transmission to the beam splitter BS1 the same unitary polarization transformation. To achieve this, we first replace one detector by the polarimeter,

set the switch to send light through the path of verifier 0, and record the polarization state. Then we set the switch to direct light through the verifier 1 path, and adjust the polarization modulator PM1 such that the same polarization state is obtained. In this way we calibrate the transmission through the full setup and we do not have to change any fiber connections after this calibration, which avoids unavoidable drifts after reconnecting or moving a fiber. The fidelity of the produced polarization states is around 99.9%, it degrades by a few percent during the measurements, most likely due to temperature fluctuations.

Prover

To realize the SWAP protocol, the prover uses a system of 3 fiber-based beam splitters (Thorlabs TW930R5A2) in combination with four avalanched single-photon detectors labeled A-D in Fig. 6.2 (Excelitas SPCM-AQRH-14-FC-ND). We use a time-tagging card (Cronologic HPTDC, 100 ps resolution) and custom software to record all single counts and all combinations of 2-, 3-, and 4-fold coincidence detection events within a 1 ns time window (see Appendix 6.7.3 for details). From these coincidence events, the prover determines their answer, and reports a conclusive result if exactly two photons are detected - otherwise, if less or more than 2 photons are detected, which can happen due to loss or dark counts, an inclusive result is reported: $z = \oslash$. If conclusive, the prover wants to determine if the polarization of both photons is equal or not, for which the HOM effect is used - equal photons "bunch" and exit beam splitter BS1 through the same output port. In this case detectors AB or CD click and the prover returns $z = 0$. Otherwise, if detectors AC, AD, BC or BD click, HOM photon bunching did not happen and the prover returns $z = 1$.

6.4 Results

The experimental procedure is as follows: (i) We calibrate the polarization of the setup as described above, and record the settings. (ii) The single-photon source is optimized (laser power, polarization, quantum dot bias voltage). (iii) Data is recorded for 5-minute intervals. Steps (ii) and (iii) are repeated for the measurement time. Fig. 6.3 shows the raw and normalized coincidence events. We focus here on only one polarization basis, the HV basis. We note that we observe no 3- and 4-fold events in our one-hour long measurements.

If our experiment would be perfect, all coincidence events are equally probable for orthogonal qubits ($\perp$) from the verifiers. This is well recognizable in Fig. 6.3, red bars. If the qubits from the verifiers are equal ($\parallel$), we would expect perfect HOM photon bunching and that only AB and CD events appear. In Fig. 6.3(a), we indeed observe an enhancement of these events, but also a rather large amount of unexpected coincidences (AC,AD,BC,BD), which we will discuss below. In Fig. 6.3(b) we show the normalized coincidences

$$CC_{ij}^{norm} = \frac{CC_{ij}}{SC_i\, SC_j} \tag{6.1}$$

where CC_{ij} are the two-photon coincidence events of detectors i and j, and SC_i are the single-photon detection events of detector i. This shows that the large difference between

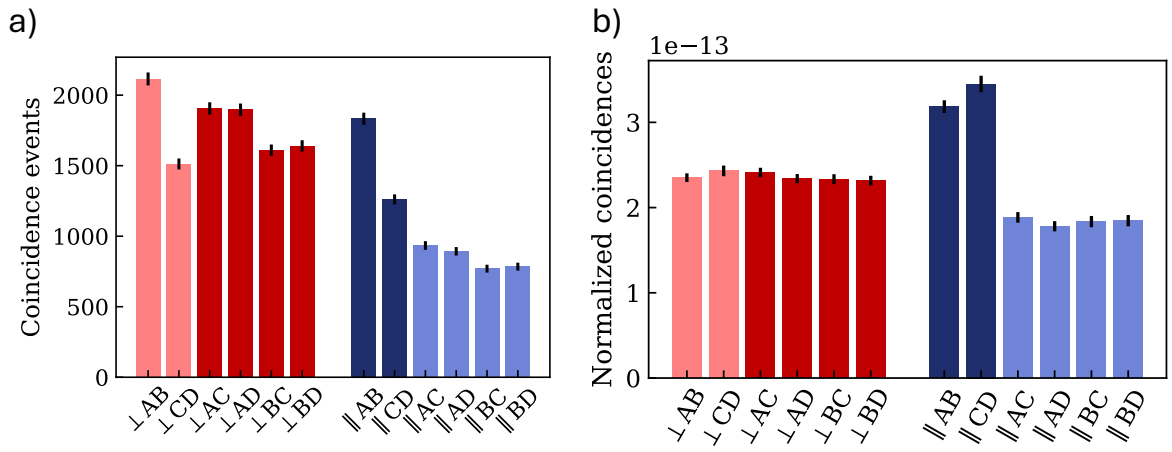


Figure 6.3: Photon correlations at the prover, raw coincidences CC_{ij} (a) and normalized coincidences CC_{ij}^{norm} (b) for a 5 hour long measurement. For orthogonal verifier qubits ($\perp$, red), theory predicts equal rates which is well reproduced in the experiment. For parallel qubits ($\|$, blue), only $\|$AB and $\|$CD events are expected - the unwanted events are due to imperfections of our single-photon source as explained in the text. The error bars indicate the statistical uncertainties assuming uncorrelated errors (shot noise).

	Theory	Experiment
$\mathbb{P}(\oslash \mid \perp)$	1/4	NA
$\mathbb{P}(\oslash \mid \|)$	1/2	NA
$\mathbb{P}(0 \mid \perp, \text{concl.})$	1/3	0.34 ± 0.01
$\mathbb{P}(1 \mid \perp, \text{concl.})$	2/3	0.66 ± 0.01
$\mathbb{P}(0 \mid \|, \text{concl.})$	1	0.48 ± 0.01
$\mathbb{P}(1 \mid \|, \text{concl.})$	0	0.52 ± 0.01

Table 6.1: Expected and measured probabilities, and their statistical errors (shot noise).

$CC^{\parallel}_{AB}$ and $CC^{\parallel}_{CD}$ in Fig. 6.3(a) originates from unbalanced beam splitters and different transmissions of the respective paths, which is removed by this normalization.

6.4.1 Prover answers

The prover determines the answer from the photon detection events as explained above and in the final step in the verification process the verifiers check if the conclusive responses from the prover follow the expected distribution. This is done by calculating the ratio of correct and incorrect answers received from the prover. We now discuss the expected results, and compare to the experimental data. The results are shown in Table 6.1 and Fig. 6.4.

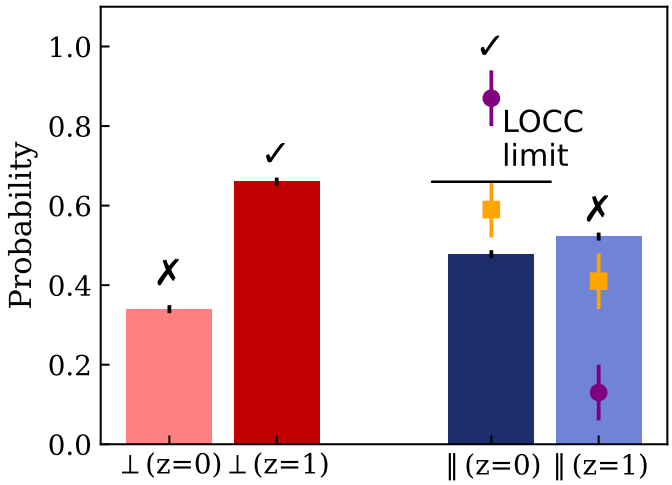


Figure 6.4: Conditional probabilities of prover response for both orthogonal ($\perp$) and parallel ($\parallel$) qubits sent from the verifiers, conditioned on the response being conclusive. The dark colored bars indicate a 'correct' (✓) response from the prover while the light color indicates an 'incorrect' answer (✘). The probability of $z = 0$ is obtained from the sum of AB and CD coincidences and the probability for $z = 1$ is determined from the sum of the other four 2-fold coincidences. To obtain probabilities, both are divided by the total amount of 2-fold coincidences. The 'LOCC limit' of 2/3 is the maximal achievable probability for attackers under the LOCC assumption. Symbols show predictions for our setup but using an improved single-photon source (orange squares for only an improved purity, purple circles for improved purity and indistinguishability).

First, what is the probability to obtain an inconclusive result, where the two photons are absorbed by the same detector – for the case of an ideal experiment without loss? In the case of orthogonal qubits ($\perp$) where no HOM photon bunching is happening, the chance that both photons leave the beam splitter through the same port is 1/2, and this must happen twice, at BS1 and then at BS2 or BS3 - therefore $\mathbb{P}(\oslash|\ \perp)$=1/4. In the case of parallel qubits ($\parallel$), HOM photon bunching happens at BS1 with certainty, and therefore the chance of an inconclusive result is twice as high: $\mathbb{P}(\oslash|\ \parallel) = 1/2$.

Now, we discuss the different probabilities conditioned on a conclusive answer, i.e., that two photons were detected. For the case of orthogonal qubits ($\perp$) arriving from the

verifiers, since no HOM photon bunching happens, all 6 coincidence events are equally probable. We obtain $\mathbb{P}(0|\perp, \text{concl.}) = 2/6 = 1/3$ and $\mathbb{P}(1|\perp, \text{concl.}) = 4/6 = 2/3$. This is important, also in the ideal case, the prover will return the 'wrong' answer $z = 0$ that should indicate parallel qubits. Finally, for parallel $\|$ qubits, the photons exit BS1 through the same port as a consequence of HOM photon bunching, only AB and CD coincidences can occur which results in $z = 0$ and consequently $\mathbb{P}(0|\,\|, \text{concl.}) = 1$.

These expectations and the experimental results calculated from the data in Fig. 6.3 are shown in Table 6.1 and Fig. 6.4. We see that the mentioned unexpected coincidences (AC,AD,BC,BD for $\|$ qubits) results in a non-zero $\mathbb{P}(1|\,\|, \text{concl.})$, which by normalization ($\mathbb{P}(0|\,\|, \text{concl.}) + \mathbb{P}(1|\,\|, \text{concl.}) = 1$) results in a reduced $\mathbb{P}(0|\,\|, \text{concl.})$. Before discussing the origin of this deviation from expectation, we now discuss the theoretical bound for secure QPV.

6.4.2 LOCC attack

We now sketch which best-case probabilities two adversaries can obtain, if they are restricted to LOCC. Every round, each adversary intercepts (see Fig. 6.1) the qubit sent by the verifier closest to them and measures it in a certain basis (diamonds in Fig. 6.1). Then, they share their results with the other adversary and formulate a response that is sent to the verifiers (circles in Fig. 6.1). Assuming that the verifiers use all three mutually unbiased bases, there is a 1/3 probability that the adversaries have measured in the correct basis which enables them to return the correct expected result with certainty. For the other two basis choices (each also occurring with a 1/3 probability), there is still a chance of 1/2 to guess correctly the answer, therefore we obtain as the correct-guessing probability of the LOCC adversaries

$$\mathbb{P}_{\text{succes}}^{\text{LOCC}} = \frac{1}{3}\left(1 + \frac{1}{2} + \frac{1}{2}\right) = \frac{2}{3}. \tag{6.2}$$

A proper proof for this bound is given in Ref. [18]. As mentioned before, even in an ideal experiment and without adversaries, for orthogonal qubits, the result is correct with only a chance of 2/3. Since, however, ideally, equal amounts of rounds are played with orthogonal and parallel qubits, where the latter results always in the correct answer, the correct answer is sent with probability 5/6.

6.5 Discussion

For orthogonal qubits ($\perp$) the measurement data follows the expected distribution where 2/3 of the time the honest prover responds correctly as seen in Fig. 6.4, and we conclude that differences in efficiencies in the setup are not significant for the prover responses in this case. For parallel ($\|$) qubits, as we have mentioned, our data deviates from the expectations, the origin of this we explore now.

We have made a simple model of our experiment including photon source parameters, and all characteristics of the optical setup including loss, unbalanced fiber beam splitters, and detection efficiencies, a detailed characterization is given in Appendix 6.7.1. The single-photon source is characterized by the single-photon purity P and the photon indistinguishability or wave-function overlap M [66, 67, 75, 76] - because our protocol is loss-resilient, we ignore the single-photon brightness here. The single-photon purity P

is given by $P = 1 - g^{(2)}$ where the zero-time second-order correlation function $g^{(2)}$ is measured in a Hanbury Brown and Twiss (HBT) experiment. To obtain the wavefunction overlap M, we first measure in a HOM experiment the zero-time second-order HOM correlation functions for orthogonal ($g_{\perp}^{(2)}$) and parallel ($g_{\parallel}^{(2)}$) polarized photons. From this, the interferometric HOM visibility $\mathcal{V}_{HOM}$ can be calculated from [62, 100].

$$\mathcal{V}_{HOM} = \frac{g_{\perp}^{(2)} - g_{\parallel}^{(2)}}{g_{\perp}^{(2)}}. \tag{6.3}$$

Now we can calculate the bare photon indistinguishability or wave-function overlap from [62]:

$$M = \mathcal{V}_{HOM} \left(1 + g^{(2)}\right), \tag{6.4}$$

which shows that the interferometric visibility $\mathcal{V}_{HOM}$ is reduced by a non-ideal single-photon purity.

For our source, we measure $g_{\parallel}^{(2)} = (36.8 \pm 3.0)\%$ and $g_{\perp}^{(2)} = (58.8 \pm 3.6)\%$, resulting in a interferometric visibility of $\mathcal{V}_{HOM} = (37.4 \pm 6.4)\%$ and an indistinguishability of $M = (45.8 \pm 10.1)\%$. To figure out the origin of these non-ideal results, and to identify where our experiment can most easily be improved, we use our model to predict the most critical QPV probability $\mathbb{P}(0|\ \|, \text{concl.})$, i.e. that the prover answers $z = 0$ on parallel inputs $|\Psi_0\rangle\ \|\ |\Psi_1\rangle$. We use all our experimental details but alter the single-photon performance metrics - using experimental data from an excellent single-photon source by Tomm et al. [66]. We consider two cases in addition to ours (A), first using all metrics from Tomm et al. (B), and then only their single-photon purity but our indistinguishability (C). In each case, indistinguishability data of photons produced 1 µs apart are used. All results are shown in Table 6.2. We see that a near-ideal single-photon source (case B, also indicated by the purple symbol in Fig. 6.4) is sufficient to clearly exceed the threshold of $\mathbb{P}(0|\ \|, \text{concl.}) = 2/3$, but also just an improved purity would bring our experiment closer to this threshold (case C, orange symbol in Fig. 6.4). In our case, this is caused by non-resonant background emission, finite cross-polarization laser extinction [104], and by re-excitation of the quantum dot since the length of the excitation pulse was similar to the QD lifetime of around 100 ps [72].

	Our work (A)	Tomm et al. (B)	Mix (C)
Purity P	0.776 ± 0.017	0.979 ± 0.001	0.979 ± 0.001
$g_{\parallel}^{(2)}$	0.368 ± 0.030		
$g_{\perp}^{(2)}$	0.588 ± 0.036		
$\mathcal{V}_{HOM}$	0.374 ± 0.064	0.940 ± 0.001	0.448 ± 0.100
M	0.458 ± 0.101	0.960 ± 0.005	0.458 ± 0.101
$\mathbb{P}(0\|\ \|, \text{concl.})$	0.47 ± 0.03	0.890 ± 0.003	0.55 ± 0.06

Table 6.2: Overview of the parameters and resulting conditional probability $\mathbb{P}(0|\ \|, \text{concl.})$ for our single-photon source (A), the source presented in Tomm et. al. (B, [66]) and for a source similar to our (A) but with improved single-photon purity (C). The derivation of the correlation values and uncertainties is explained in Appendix 6.7.3.

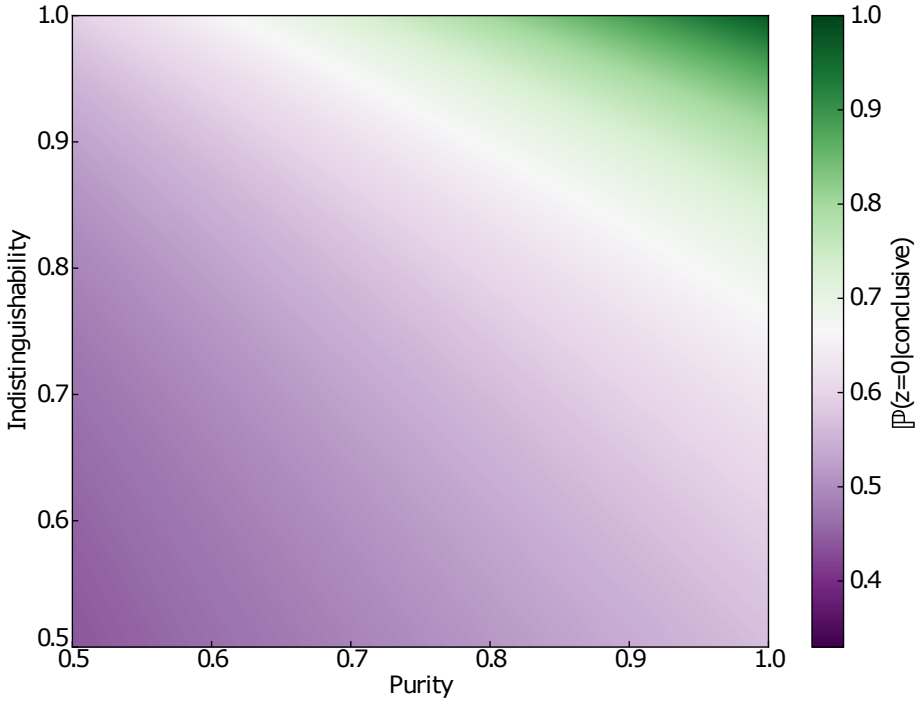


Figure 6.5: Probability of a correct $z = 0$ response $\mathbb{P}(0|\ \|, \text{concl.})$ depending on single-photon purity and indistinguishability using otherwise our experimental parameters. The white line marks the threshold of 2/3 above which (green) a LOCC attack is not successful.

We show in Fig. 6.5 how the probability $\mathbb{P}(0|\ \|, \text{concl.})$ depends on the single-photon purity and indistinguishability, where otherwise our experimental parameters and inaccuracies given in Appendix 6.7.1 are used. We see that both purity and indistinguishability need to be high to exceed the threshold of 2/3.

Finally, although the initial polarization state fidelity at the prover is very high, this fidelity can decrease by around a few percent during the measurements, most likely by temperature fluctuations of the 200 m long fiber. This decreases the wave-function overlap by a similar amount and with this the HOM visibility.

6.6 Conclusions and outlook

We have shown first experimental results for a loss-tolerant quantum position verification protocol, using a temporally demultiplexed quantum dot - microcavity based single-photon source. We found that the Hong-Ou-Mandel visibility of our single-photon source is the limiting factor to reach the threshold for quantum secure discrimination between a honest prover and adversaries that are restricted to local operations and classical communication (LOCC), i.e., not having shared entanglement. We also found that with an improved single-photon source, this threshold is within reach - the single-photon purity and indistinguishability can be improved by using shorter excitation pulses to avoid re-excitation and improve the wave-function overlap, and improved cross-polarization to avoid contamination of the single-photon pulses by the excitation laser.

For future research, next to improvements of the single-photon source, we stress that, addressing the slow quantum information loophole is most urgent as it would allow using

existing fiber networks, and a promising candidate is a functional single-photon QPV protocol [23] in combination with a commitment step [19].

6.7 Appendix

6.7.1 Experimental setup characterization

Here we present a precise characterization of the experimental setup, which is crucial for the model used in the main text. For this, we directly connected a continuous-wave (CW) laser to the input of the fiber switch using the wavelength of the single photons (around 935 nm) and measure the intensity of the laser light at every fiber connection with a power meter (Thorlabs PM100D with sensor S130C). The position of every fiber connection is depicted in Fig. 6.6 and the measured transmission ratios are shown in Table 6.3. For intensity measurements behind BS1, we blocked the beam in the free-space delay stage to avoid interference effects. The transmission ratios given for the beam splitters (BS1, BS2 and BS3) are the ratios between the input intensity and the sum of the intensities at the two outputs of the beam splitter. The splitting ratios are presented in Table 6.4. The overall efficiency of the system is between 7.2% and 12.4% and depends on the path taken and detection efficiency of the detectors.

The nonlinearity of power measurements used for determination of the transmissions is ±0.5 % and are therefore negligible.

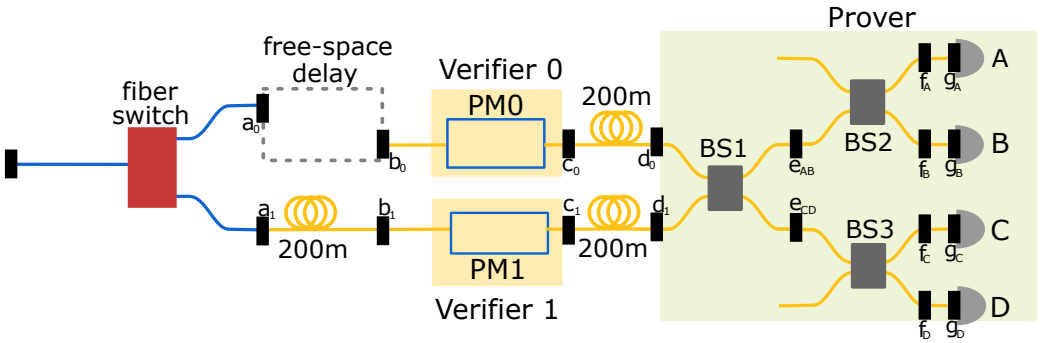


Figure 6.6: Sketch of a part of the experimental setup with labels indicating the measurement points for the characterization.

	Transmission (%)	Transmission (%)
	Verifier 0	Verifier 1
after switch	71.2	60.3
delay stage	95.4	91.5
polarization modulator (PM)	81.4	89.4
200m fiber transmission	86.2	85.2
total (a-d)	47.7	42.0
BS1* (e)	94.9	
BS2* ($f_{A/B}$)	99.7	
BS3* ($f_{C/D}$)	86.8	
detector A fiber (g_A)	90.6	
detector A efficiency**	100	
detector B fiber (g_B)	90.3	
detector B efficiency**	61.9	
detector C fiber (g_C)	90.7	
detector C efficiency**	68.9	
detector D fiber (g_D)	97.9	
detector D efficiency**	15.9	

Table 6.3: Overview of relative transmissions for each component in the experimental setup as shown in Fig. 6.6. The loss of the fiber-based beam splitters (*) is measured as the ratio between the input of the beam splitter and the sum of the two outputs. The splitting ratios themselves are described in Table 6.4. All detector efficiencies (**) are normalized to that of detector A since for the analysis in the main text only relative efficiencies are relevant. From multiple measurements, we estimate the errors on the values to be about 1-2 %, but we note that e.g. fiber coupling efficiencies between fiber reconnects can vary randomly by up to 5 %.

beam splitter	Ratio upper output (%)	Ratio lower output (%)
BS1 (d_1)	54.5 (e_{AB})	45.5 (e_{CD})
BS2 (e_{AB})	44.1 (f_A)	55.9 (f_B)
BS3 (e_{CD})	53.0 (f_C)	47.0 (f_D)

Table 6.4: Overview of the splitting ratios of the fiber-based beam splitters (Thorlabs TW930R5A2), not accounting for the total loss in transmission described in Table 6.3. The labels in brackets denotes between which points in the setup the ratios were measured. Statistical measurement errors are around 1-2%.

6.7.2 Measured coincidence events and normalized coincidences

	Coincidence events		Normalized coincidences	
	$\perp$	$\parallel$	$\perp$ /10^{-9}	$\parallel$ /10^{-9}
AB	2115	1833	0.82	1.19
CD	1512	1261	0.83	1.29
AC	1906	934	0.82	0.70
AD	1897	893	0.81	0.67
BC	1610	770	0.81	0.69
BD	1640	784	0.79	0.68

Table 6.5: Raw values for Fig. 6.3 of the main text.

6.7.3 Correlation measurements and uncertainties

Here we discuss the uncertainties of the correlation data in Table II of the main text. We calculate the second-order correlation function at zero time delay from $g^{(2)} = N_0/N$ where N_0 are the total coincidence events within a 1 ns time window at zero time delay (dark gray area in Fig. 6.7), and N is the averaged number of coincidence events of 10 side-peaks (5 to the left and 5 to the right of the zero time delay peak, light gray areas in Fig. 6.7), also within 1 ns time windows. Regarding statistical errors, these values are subject to shot noise with $\Delta N = \sqrt{N}$. By propagation of uncertainties, the error on the $g^{(2)}(0)$ is given by

$$\Delta g^{(2)}(0) = g^{(2)}(0)\sqrt{\left(\frac{\Delta N_0}{N_0}\right)^2 + \left(\frac{\Delta N}{N}\right)^2}. \tag{6.5}$$

The given values of $g^{(2)}(0)$, $g^{(2)}_{\parallel}(0)$ and $g^{(2)}_{\perp}(0)$ in column A of Table II are used to calculate the HOM visibility $\mathcal{V}_{\mathrm{HOM}}$ and the indistinguishability M, where for both the error was propagated similarly as shown in Eq. 6.5. For column B and C in Table II, the uncertainties were directly taken from the cited literature (B) or calculated as above (C).

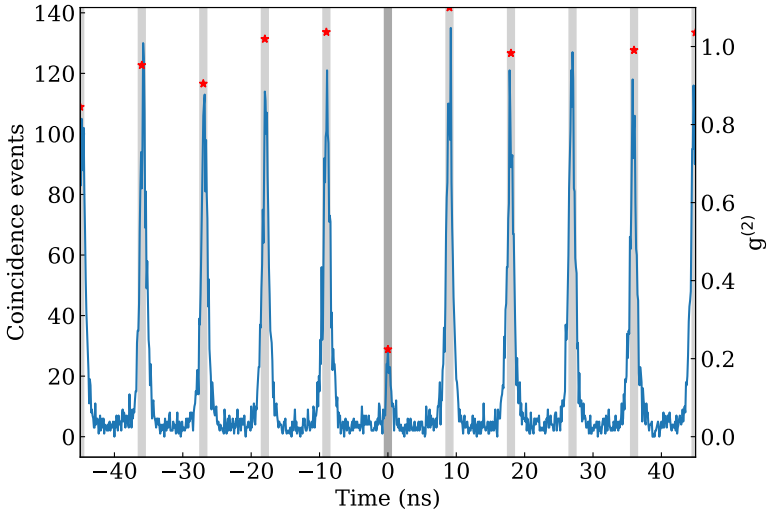


Figure 6.7: Exemplary second-order correlation function measurement of our single-photon source. The left axis shows the raw coincidence events, the dark and light gray areas indicate the time windows used for calculation of event counts, and the stars (right axis) indicate the normalized $g^{(2)}$ values.

For estimation of the uncertainties of $\mathbb{P}\,(0|\ \ \|, \text{concl.})$ shown in Table II, we use worst-case estimation based on statistical errors of $\mathcal{V}_{\text{HOM}}$.

Bibliography

[1] Chandran, N., Goyal, V., Moriarty, R. & Ostrovsky, R. Position Based Cryptography. In Halevi, S. (ed.) *Advances in Cryptology - CRYPTO 2009*, 391 (Springer, Berlin, Heidelberg, 2009).

[2] Beausoleil, R. G., Kent, A., Spiller, T. P. & Munro, W. J. Tagging Systems (2006).

[3] Kent, A. Quantum Tagging for Tags Containing Secret Classical Data. *Phys. Rev. A* **84**, 022335 (2011).

[4] Kent, A., Munro, W. J. & Spiller, T. P. Quantum Tagging: Authenticating Location via Quantum Information and Relativistic Signaling Constraints. *Phys. Rev. A* **84**, 012326 (2011).

[5] Lau, H.-K. & Lo, H.-K. Insecurity of Position-Based Quantum-Cryptography Protocols against Entanglement Attacks. *Phys. Rev. A* **83**, 012322 (2011).

[6] Malaney, R. A. Location-Dependent Communications Using Quantum Entanglement. *Phys. Rev. A* **81**, 042319 (2010).

[7] Malaney, R. A. Quantum Location Verification in Noisy Channels. In *2010 IEEE Global Telecommunications Conference GLOBECOM 2010*, 1 (2010). arXiv: 1004.4689.

[8] Qi, B. & Siopsis, G. Loss-Tolerant Position-Based Quantum Cryptography. *Phys. Rev. A* **91**, 042337 (2015).

[9] Ribeiro, J. & Grosshans, F. A Tight Lower Bound for the BB84-states Quantum-Position-Verification Protocol (2015). arXiv: 1504.07171.

[10] Unruh, D. Quantum Position Verification in the Random Oracle Model. In Garay, J. A. & Gennaro, R. (eds.) *Advances in Cryptology – CRYPTO 2014*, 1 (Springer Berlin Heidelberg, Berlin, Heidelberg, 2014).

[11] Tomamichel, M., Fehr, S., Kaniewski, J. & Wehner, S. A Monogamy-of-Entanglement Game with Applications to Device-Independent Quantum Cryptography. *New J. Phys.* **15**, 103002 (2013).

[12] Lim, C. C. W. *et al.* Loss-Tolerant Quantum Secure Positioning with Weak Laser Sources. *Phys. Rev. A* **94**, 032315 (2016).

[13] Gao, F., Liu, B. & Wen, Q.-Y. Enhanced No-Go Theorem for Quantum Position Verification (2013). arXiv: 1305.4254.

[14] Buhrman, H., Fehr, S., Schaffner, C. & Speelman, F. The Garden-Hose Model. In *Proceedings of the 4th Conference on Innovations in Theoretical Computer Science*, 145 (ACM, Berkeley California USA, 2013).

[15] Buhrman, H. *et al.* Position-Based Quantum Cryptography: Impossibility and Constructions. *SIAM J. Comput.* **43**, 150 (2014).

[16] Chakraborty, K. & Leverrier, A. Practical Position-Based Quantum Cryptography. *Phys. Rev. A* **92**, 052304 (2015).

[17] Allerstorfer, R., Buhrman, H., Speelman, F. & Lunel, P. V. On the Role of Quantum Communication and Loss in Attacks on Quantum Position Verification (2022). arXiv: 2208.04341.

[18] Allerstorfer, R., Buhrman, H., Speelman, F. & Lunel, P. V. Towards Practical and Error-Robust Quantum Position Verification (2022). arXiv: 2106.12911.

[19] Allerstorfer, R. *et al.* Making Existing Quantum Position Verification Protocols Secure Against Arbitrary Transmission Loss (2023). arXiv: 2312.12614.

[20] Allerstorfer, R., Buhrman, H., May, A., Speelman, F. & Verduyn Lunel, P. Relating Non-Local Quantum Computation to Information Theoretic Cryptography. *Quantum* **8**, 1387 (2024).

[21] Amer, O. *et al.* Certified Randomness Implies Secure Classical Position-Verification (2024). arXiv: 2410.03982.

[22] Asadi, V., Cleve, R., Culf, E. & May, A. Linear Gate Bounds against Natural Functions for Position-Verification (2024). arXiv: 2402.18648.

[23] Bluhm, A., Christandl, M. & Speelman, F. A Single-Qubit Position Verification Protocol That Is Secure against Multi-Qubit Attacks. *Nat. Phys.* **18**, 623 (2022).

[24] Cowperthwaite, G., Kent, A. & Pitalua-Garcia, D. Towards a Proof-of-Principle Experimental Demonstration of Quantum Position Verification: Working Notes (2023). arXiv: 2309.10070.

[25] Cree, J. & May, A. Code-Routing: A New Attack on Position Verification. *Quantum* **7**, 1079 (2023).

[26] Escolà-Farràs, L. & Speelman, F. Single-Qubit Loss-Tolerant Quantum Position Verification Protocol Secure against Entangled Attackers. *Phys. Rev. Lett.* **131**, 140802 (2023).

[27] Escolà-Farràs, L., Palais, L. C. & Speelman, F. A Quantum Cloning Game with Applications to Quantum Position Verification (2024). arXiv: 2410.22157.

[28] Escolà-Farràs, L. & Speelman, F. Quantum Position Verification in One Shot: Parallel Repetition of the f-BB84 and f-Routing Protocols (2025). arXiv: 2503.09544.

[29] Escolà-Farràs, L. & Speelman, F. Lossy-and-Constrained Extended Non-Local Games with Applications to Quantum Cryptography. *Quantum* **9**, 1712 (2025). arXiv: 2405.13717.

[30] George, I., Allerstorfer, R., Lunel, P. V. & Chitambar, E. Orthogonality Broadcasting and Quantum Position Verification (2024). arXiv: 2311.00677.

[31] Junge, M., Kubicki, A. M., Palazuelos, C. & Pérez-García, D. Geometry of Banach Spaces: A New Route Towards Position Based Cryptography. *Commun. Math. Phys.* **394**, 625 (2022).

[32] Liu, J., Liu, Q. & Qian, L. Beating Classical Impossibility of Position Verification (2022). arXiv: 2109.07517.

[33] May, A. Quantum Tasks in Holography. *J. High Energy Phys.* **2019**, 233 (2019).

[34] Miller, C. A. & Alnawakhtha, Y. Perfect Cheating Is Impossible for Single-Qubit Position Verification (2024). arXiv: 2406.20022.

[35] Olivo, A., Chabaud, U., Chailloux, A. & Grosshans, F. Breaking Simple Quantum Position Verification Protocols with Little Entanglement (2020). arXiv: 2007.15808.

[36] Bennett, C. H. & Brassard, G. Quantum Cryptography: Public Key Distribution and Coin Tossing. *Theor. Comput. Sci.* **560**, 7 (2014).

[37] Hong, C. K., Ou, Z. Y. & Mandel, L. Measurement of Subpicosecond Time Intervals between Two Photons by Interference. *Phys. Rev. Lett.* **59**, 2044 (1987).

[38] Garcia-Escartin, J. C. & Chamorro-Posada, P. Swap Test and Hong-Ou-Mandel Effect Are Equivalent. *Phys. Rev. A* **87**, 052330 (2013).

[39] Poletti, F. *et al.* Towards High-Capacity Fibre-Optic Communications at the Speed of Light in Vacuum. *Nat. Photonics* **7**, 279 (2013).

[40] Antesberger, M. *et al.* Distribution of Telecom Entangled Photons through a 7.7 Km Antiresonant Hollow-Core Fiber. *Opt. Quantum* **2**, 173 (2024).

[41] Petrovich, M. *et al.* Broadband Optical Fibre with an Attenuation Lower than 0.1 Decibel per Kilometre. *Nat. Photonics* 1 (2025).

[42] Damask, J. N. *Polarization optics in telecommunications*. No. 101 in Springer series in optical sciences (Springer, New York, 2005).

[43] Jozsa, R. Fidelity for Mixed Quantum States. *Journal of Modern Optics* **41**, 2315 (1994).

[44] Ren, Z. B., Robert, Ph. & Paratte, P.-A. Temperature Dependence of Bend- and Twist-Induced Birefringence in a Low-Birefringence Fiber. *Opt. Lett.* **13**, 62 (1988).

[45] Rodimin, V. *et al.* Impact of Polarization Mode Dispersion on Entangled Photon Distribution (2025). arXiv: 2408.01754.

[46] Poole, C. & Wagner, R. Phenomenological Approach to Polarisation Dispersion in Long Single-Mode Fibres. *Electron. Lett.* **22**, 1029 (1986).

[47] Jopson, R., Nelson, L. & Kogelnik, H. Measurement of Second-Order Polarization-Mode Dispersion Vectors in Optical Fibers. *IEEE Photonics Technol. Lett.* **11**, 1153 (1999).

[48] Dong, H. *et al.* Generalized Mueller Matrix Method for Polarization Mode Dispersion Measurement in a System with Polarization-Dependent Loss or Gain. *Opt. Express* **14**, 5067 (2006).

[49] Brodsky, M., Frigo, N. J., Boroditsky, M. & Tur, M. Polarization Mode Dispersion of Installed Fibers. *J. Lightwave Technol.* **24**, 4584 (2006).

[50] Hakki, B. Polarization Mode Dispersion in a Single Mode Fiber. *J.Lightwave Technol.* **14**, 2202 (1996).

[51] Galtarossa, A., Gianello, G., Someda, C. & Schiano, M. In-Field Comparison among Polarization-Mode-Dispersion Measurement Techniques. *J. Lightwave Technol.* **14**, 42 (1996).

[52] Heffner, B. Automated Measurement of Polarization Mode Dispersion Using Jones Matrix Eigenanalysis. *IEEE Photonics Technol. Lett.* **4**, 1066 (1992).

[53] Poole, C. D. Measurement of Polarization-Mode Dispersion in Single-Mode Fibers with Random Mode Coupling. *Opt. Lett.* **14**, 523 (1989).

[54] Rashleigh, S. C. & Ulrich, R. Polarization Mode Dispersion in Single-Mode Fibers. *Opt. Lett.* **3**, 60 (1978).

[55] Czegledi, C. B., Karlsson, M., Agrell, E. & Johannisson, P. Polarization Drift Channel Model for Coherent Fibre-Optic Systems. *Sci. Rep.* **6**, 21217 (2016).

[56] Ramos, M. F., Pinto, A. N. & Silva, N. A. Polarization Based Discrete Variables Quantum Key Distribution via Conjugated Homodyne Detection. *Sci. Rep.* **12**, 6135 (2022).

[57] Maring, N. *et al.* A Versatile Single-Photon-Based Quantum Computing Platform. *Nat. Photonics* **18**, 603 (2024).

[58] Li, Y.-H. *et al.* Free-Space and Fiber-Integrated Measurement-Device-Independent Quantum Key Distribution under High Background Noise. *Phys. Rev. Lett.* **131**, 100802 (2023).

[59] Semenenko, H., Sibson, P., Thompson, M. G. & Erven, C. Interference between Independent Photonic Integrated Devices for Quantum Key Distribution. *Opt. Lett.* **44**, 275 (2019).

[60] Santori, C., Fattal, D., Vučković, J., Solomon, G. S. & Yamamoto, Y. Indistinguishable Photons from a Single-Photon Device. *Nature* **419**, 594 (2002).

[61] Patel, R. B. *et al.* Quantum Interference of Electrically Generated Single Photons from a Quantum Dot. *Nanotechnology* **21**, 274011 (2010).

[62] Patel, R. B. *et al.* Postselective Two-Photon Interference from a Continuous Nonclassical Stream of Photons Emitted by a Quantum Dot. *Phys. Rev. Lett.* **100**, 207405 (2008).

[63] Proux, R. *et al.* Measuring the Photon Coalescence Time Window in the Continuous-Wave Regime for Resonantly Driven Semiconductor Quantum Dots. *Phys. Rev. Lett.* **114**, 067401 (2015).

[64] Wenniger, I. M. d. B. *et al.* Quantum Interferences and Gates with Emitter-Based Coherent Photon Sources. *Optica Quantum* **2**, 404 (2024). arXiv: `2401.01187`.

[65] Ates, S. *et al.* Post-Selected Indistinguishable Photons from the Resonance Fluorescence of a Single Quantum Dot in a Microcavity. *Phys. Rev. Lett.* **103**, 167402 (2009).

[66] Tomm, N. *et al.* A Bright and Fast Source of Coherent Single Photons. *Nat. Nanotechnol.* **16**, 399 (2021).

[67] Ding, X. *et al.* High-Efficiency Single-Photon Source above the Loss-Tolerant Threshold for Efficient Linear Optical Quantum Computing. *Nat. Photonics* **19**, 387 (2025).

[68] Wenniger, I. M. d. B. *Impact of Photon-Number Coherence on the Performance and Energetics of Quantum Optics Protocols*. Ph.D. thesis, Université Paris-Saclay (2023).

[69] Loredo, J. C. *et al.* Generation of Non-Classical Light in a Photon-Number Superposition. *Nat. Photonics* **13**, 803 (2019).

[70] Wein, S. C. *et al.* Photon-Number Entanglement Generated by Sequential Excitation of a Two-Level Atom. *Nat. Photonics* **16**, 374 (2022).

[71] Steindl, P. *et al.* Artificial Coherent States of Light by Multiphoton Interference in a Single-Photon Stream. *Phys. Rev. Lett.* **126**, 143601 (2021).

[72] Poortvliet, M. *et al.* Picosecond Laser Pulses for Quantum Dot–Microcavity-Based Single-Photon Generation by Cascaded Electro-Optic Modulation of a Narrow-Linewidth Laser. *Phys. Rev. Appl.* **23**, 014017 (2025).

[73] Paudel, U. *et al.* Generation of Frequency Sidebands on Single Photons with Indistinguishability from Quantum Dots. *Phys. Rev. A* **98**, 011802 (2018).

[74] Zhai, L. *et al.* Quantum Interference of Identical Photons from Remote GaAs Quantum Dots. *Nat. Nanotechnol.* **17**, 829 (2022).

[75] Somaschi, N. *et al.* Near-Optimal Single-Photon Sources in the Solid State. *Nat. Photonics* **10**, 340 (2016).

[76] Thomas, F. S. *et al.* Spectroscopy of the Local Density of States in Nanowires Using Integrated Quantum Dots. *Phys. Rev. B* **104**, 115415 (2021).

[77] Snijders, H. J. *et al.* Observation of the Unconventional Photon Blockade. *Phys. Rev. Lett.* **121**, 043601 (2018).

[78] Steindl, P. *et al.* Cross-Polarization-Extinction Enhancement and Spin-Orbit Coupling of Light for Quantum-Dot Cavity Quantum Electrodynamics Spectroscopy. *Phys. Rev. Appl.* **19**, 064082 (2023).

[79] Steindl, P. *et al.* Resonant Two-Laser Spin-State Spectroscopy of a Negatively Charged Quantum-Dot–Microcavity System with a Cold Permanent Magnet. *Phys. Rev. Appl.* **20**, 014026 (2023).

[80] Istrati, D. *et al.* Sequential Generation of Linear Cluster States from a Single Photon Emitter. *Nat. Commun.* **11**, 5501 (2020).

[81] Guichard, V. *et al.* Monitoring the Generation of Photonic Linear Cluster States with Partial Measurements (2025). arXiv: 2505.01929.

[82] Bienfang, J. *et al.* Single-Photon Sources and Detectors Dictionary. Tech. Rep., National Institute of Standards and Technology (U.S.) (2023).

[83] Couteau, C. Spontaneous Parametric Down-Conversion. *Contemp. Phys.* **59**, 291 (2018).

[84] Eisaman, M. D., Fan, J., Migdall, A. & Polyakov, S. V. Invited Review Article: Single-photon Sources and Detectors. *Rev. Sci. Instrum.* **82**, 071101 (2011).

[85] Wang, H. *et al.* Bright Heralded Single-Photon Source Saturating Theoretical Single-photon Purity. *Laser Photonics Rev.* **19**, 2401420 (2025). arXiv: 2404.03236.

[86] Loredo, J. C. *et al.* Scalable Performance in Solid-State Single-Photon Sources. *Optica* **3**, 433 (2016).

[87] Lenzini, F. *et al.* Active Demultiplexing of Single Photons from a Solid-State Source. *Laser Photonics Rev.* **11**, 1600297 (2017).

[88] Wang, H. *et al.* High-Efficiency Multiphoton Boson Sampling. *Nat. Photonics* **11**, 361 (2017).

[89] Kanneworff, K. *et al.* Towards Experimental Demonstration of Quantum Position Verification Using Single Photons. *Quantum Sci. Technol.* **10**, 045004 (2025).

[90] Soref, R. Tutorial: Integrated-photonic Switching Structures. *APL Photonics* **3**, 021101 (2018).

[91] Errando-Herranz, C. *et al.* MEMS for Photonic Integrated Circuits. *IEEE J. Sel. Top. Quantum Electron.* **26**, 1 (2020).

[92] Wooten, E. *et al.* A Review of Lithium Niobate Modulators for Fiber-Optic Communications Systems. *IEEE J. Sel. Top. Quantum Electron.* **6**, 69 (2000).

[93] Chen, X., Lin, J. & Wang, K. A Review of Silicon-Based Integrated Optical Switches. *Laser Photonics Rev.* **17**, 2200571 (2023).

[94] Müller, H. Fast High-Voltage Amplifiers for Driving Electro-Optic Modulators. *Rev. Sci. Instrum.* **76**, 084701 (2005).

[95] Dryazgov, M. *et al.* Resource-Efficient Low-Loss Four-Channel Active Demultiplexer for Single Photons. *Opt. Quantum* **1**, 14 (2023).

[96] Antón, C. *et al.* Interfacing Scalable Photonic Platforms: Solid-State Based Multi-Photon Interference in a Reconfigurable Glass Chip. *Optica* **6**, 1471 (2019).

[97] Münzberg, J. *et al.* Fast and Efficient Demultiplexing of Single Photons from a Quantum Dot with Resonantly Enhanced Electro-Optic Modulators. *APL Photonics* **7**, 070802 (2022).

[98] Hansen, L. M. *et al.* Single-Active-Element Demultiplexed Multi-Photon Source. *Opt. Quantum* **1**, 1 (2023).

[99] Hummel, T. *et al.* Efficient Demultiplexed Single-Photon Source with a Quantum Dot Coupled to a Nanophotonic Waveguide. *Appl. Phys. Lett.* **115**, 021102 (2019).

[100] Ollivier, H. *et al.* Hong-Ou-Mandel Interference with Imperfect Single Photon Sources. *Phys. Rev. Lett.* **126**, 063602 (2021).

[101] Brassard, G. The Conundrum of Secure Positioning. *Nature* **479**, 307 (2011).

[102] Das, S. & Siopsis, G. Practically Secure Quantum Position Verification. *New J. Phys.* **23**, 063069 (2021).

[103] Escolà-Farràs, L. & Speelman, F. Lossy-and-Constrained Extended Non-Local Games with Applications to Cryptography: BC, QKD and QPV (2024). arXiv: 2405.13717.

[104] González-Ruiz, E. M., Bjerlin, J., Sandberg, O. A. D. & Sørensen, A. S. Two-Photon Correlations and Hong-Ou-Mandel Visibility from an Imperfect Single-Photon Source. *Phys. Rev. Appl.* **23**, 054063 (2025).

Summary

In this thesis, we present our work towards a first experimental demonstration of a quantum position verification (QPV) protocol using a temporally demultiplexed quantum dot single-photon source.

Position verification is a method of authentication that relies on verifying the prover's geographical location. In position verification multiple verifiers who trust each other are located around a person who wants to prove their position, the prover. The verifiers send information to the prover, who must perform a predefined task using all the received data and return the result. By measuring the time between sending and receiving signals, the verifiers can confirm their distance from the prover. Assuming information travels at the speed of light, the maximum possible speed, the propagation time of the signals corresponds directly to twice the distance between the verifiers and the prover.

In this thesis we show a first QPV demonstration experiment in one dimension, which can be extended to three dimensions. In the one-dimensional case there are two verifiers located on opposite sides of the prover along a straight line. Previous theoretical studies have shown that the use of quantum information is essential for secure position verification, as the no-cloning theorem prevents perfect copying of quantum states, unlike classical information.

In Chapter 2 we provide a detailed overview of several QPV protocols. These protocols can be categorized by whether they use one or two qubits per round. We compare these protocols in terms of loss tolerance, the feasibility of transmitting quantum information at velocities below the speed of light, and the amount of pre-shared entanglement required to compromise the protocol. Theoretical studies have shown that single-qubit protocols incorporating substantial classical information from all verifiers are more robust against attacks involving pre-shared entanglement. Moreover, these protocols allow quantum information to be transmitted at velocities less than the speed of light, provided that classical information does propagate at the speed of light. In contrast, two-qubit protocols are fully loss-tolerant, meaning that any level of loss cannot be exploited by adversaries to their advantage, which is crucial for implementation with real hardware.

For qubits that can travel at the speed of light, single photons generated by a quantum dot single-photon source are highly suitable candidates. In this work, quantum information is encoded in the polarization state of light. In Chapter 3 we investigate the operation and stability of the polarization modulator, which is the device used for this encoding. In addition, we examine the operation and stability of long (200 m) single-mode fibers employed to simulate photon transmission between the verifiers and the prover. For both optical components, we find that the transformations applied to the polarization state of light can be considered unitary. The fidelity of the polarization states, which quantifies the similarity between states, is used as a measure to define shifts in the polarization state of light over extended periods of time. From this analysis, we infer the stability of both the polarization modulators and long optical fibers, providing insight valuable for the design of a QPV demonstration experiment. In the final part of Chapter 3 we

investigate polarization mode dispersion in long single-mode fibers and found the impact to be negligible.

A quantum dot single-photon source emits a stream of single photons in one spatial mode. Due to the epitaxial growth process of quantum dots it is challenging to fabricate two sources that emit photons which are perfectly identical (indistinguishable). To perform the two-photon QPV protocol, interference between two single photons is required. This necessitates a method to distribute photons emitted in a single spatial mode across at least two spatial modes. Furthermore, we needed to characterize the degree of single-photon indistinguishability of our quantum dot single-photon source. These questions are addressed in Chapters 4 and 5.

In Chapter 4 the stream of single photons is distributed probabilistically over two paths using a Mach-Zehnder interferometer (MZI) with an optical path length difference to interfere photons created at different times. In this chapter, we investigate not only the indistinguishability of our single-photon source but also the correlations observed at a delay corresponding to the internal delay of the interferometer. We provide both an intuitive explanation for the origin of these correlations and a system of equations describing the correlations at all possible delays. This theoretical framework yields an expression for the single-photon indistinguishability that accounts for intensity imbalances in the MZI and imperfections in the polarization-state preparation of the photons. The validity of this analytical model is verified against experimental data obtained for MZIs with both short (9 ns) and long (1 μs) internal delays.

In Chapter 5, we investigate a more deterministic distribution of single photons over two spatial modes with the use of an optical fiber switch. We provide a didactic explanation of how demultiplexing affects the single-photon stream and, consequently, the measured correlations. We find that the normalization of the second-order correlation function must be performed carefully, particularly when the switching time is only slightly longer than the interval between consecutive photons. Finally, we present the measured correlations for our quantum dot source demultiplexed with a switching time of 1 μs, showing that for slow switching the normalization error can be considered negligible.

In the final chapter of this thesis, we integrate the findings from the previous chapters to advance towards an experimental demonstration of quantum position verification. For this demonstration, we selected the two-photon SWAP protocol because of its fully loss-tolerant characteristics. The results revealed that the Hong-Ou-Mandel (HOM) visibility of our single-photon source is the limiting factor, preventing us from reaching the threshold required to differentiate between an honest prover and adversaries operating under conditions of local operations and classical communication (LOCC). However, modeling the experimental conditions in combination with a state-of-the-art single-photon source reported in literature indicates that the LOCC threshold is within reach.

Further research should involve experiments using state-of-the-art single-photon sources and continued improvements of the same protocol. More importantly, ongoing progress in the field is essential to develop QPV protocols that require fewer quantum resources, allow the transmission of quantum information at velocities below the speed of light, and remain fully tolerant to loss.

Samenvatting

In dit proefschrift presenteren we ons werk voor een eerste experimentele demonstratie van een quantum positieverificatieprotocol (QPV) met behulp van een temporeel gedemultiplexte quantum dot één-foton bron.

Positieverificatie is een authenticatiemethode die gebaseerd is op het verifiëren van de geografische locatie van de bewijzer. Bij positieverificatie bevinden zich meerdere controleurs, die elkaar vertrouwen, rondom de persoon die zijn positie wil bewijzen: de bewijzer. De controleurs sturen informatie naar de bewijzer, die een vooraf bepaalde taak moet uitvoeren met behulp van alle ontvangen gegevens en vervolgens het resultaat moet terugsturen. Door de tijd tussen het verzenden en ontvangen van signalen te meten, kunnen de controleurs hun afstand tot de bewijzer bevestigen. Ervan uitgaande dat informatie zich met de snelheid van het licht voortbeweegt, de maximaal mogelijke snelheid, komt de voortplantingstijd van de signalen rechtstreeks overeen met tweemaal de afstanden tussen de controleurs en de bewijzer.

In dit proefschrift tonen we een eerste QPV-demonstratie-experiment in één dimensie, dat kan worden uitgebreid naar drie dimensies. In het eendimensionale geval bevinden twee controleurs zich aan weerszijden van de bewijzer langs een rechte lijn. Eerdere theoretische studies hebben aangetoond dat het gebruik van quantum informatie essentieel is voor veilige positiebepaling, aangezien de no-cloning-stelling het perfect kopiëren van quantum toestanden verhindert. Dit staat in contrast met klassieke informatie, die wel perfect kan worden gekopieerd.

In hoofdstuk 2 geven we een gedetailleerd overzicht van verschillende QPV-protocollen. Deze protocollen kunnen worden gecategoriseerd op basis van het aantal qubits, één of twee, wat ze per ronden gebruiken. We vergelijken deze protocollen op het gebied van verliesbestendigheid, de haalbaarheid van het verzenden van quantum informatie met snelheden onder de lichtsnelheid en de hoeveelheid vooraf gedeelde verstrengeling die nodig is om het protocol te compromitteren. Theoretische studies hebben aangetoond dat één-qubitprotocollen die substantiële klassieke informatie van alle controleurs bevatten, robuuster zijn tegen aanvallen waarbij vooraf gedeelde verstrengeling wordt gebruikt. Bovendien maken deze protocollen het mogelijk om quantum informatie te verzenden met snelheden lager dan de lichtsnelheid, op voorwaarde dat klassieke informatie zich wel met de lichtsnelheid voortplant. Twee-qubit-protocollen zijn daarentegen volledig verliesbestendig. Dit betekent dat vijanden geen enkel verliesniveau in hun voordeel kunnen uitbuiten, wat cruciaal is voor de implementatie met echte hardware.

Voor qubits die zich met de snelheid van het licht kunnen verplaatsen, zijn enkele fotonen die worden gegenereerd door een quantum dot één-foton bron zeer geschikte kandidaten. In dit werk wordt quantum informatie gecodeerd in de polarisatietoestand van licht. In hoofdstuk 3 onderzoeken we de werking en stabilitiet van polarisatiemodulatoren, de apparatuur dat voor deze codering wordt gebruikt. Daarnaast onderzoeken we de werking en stabiliteit van lange (200 m) single-mode glasvezel kabels die worden gebruikt om de fotonentransmissie tussen de controleurs en de bewijzer te simuleren. Voor

beide optische componenten stellen we vast dat de transformaties die op de polarisatietoestand van licht worden toegepast, als unitair kunnen worden beschouwd. De fideliteit van de polarisatietoestanden, die de gelijkenis tussen toestanden kwantificeert, wordt gebruikt als maatstaf om verschuivingen in de polarisatietoestand van licht over langere perioden te definiëren. Uit deze analyse leiden we de stabiliteit af van zowel de polarisatiemodulatoren als de lange optische vezels, wat waardevolle inzichten oplevert voor het ontwerp van een QPV-demonstratie-experiment. In het laatste deel van hoofdstuk 3 onderzoeken we de polarisatiemodusdispersie in lange single-mode glasvezel kabels en constateren we dat de impact verwaarloosbaar is.

Een quantum dot één-foton bron zendt een stroom van enkelvoudige fotonen uit in één ruimtelijke modus. Vanwege het epitaxiale groeiproces van quantum dots is het een uitdaging om twee bronnen te fabriceren die fotonen uitzenden die perfect identiek (niet te onderscheiden) zijn. Om het twee-foton QPV-protocol uit te voeren, is interferentie tussen twee enkele fotonen vereist. Hiervoor is een methode nodig om fotonen die in één ruimtelijke modus worden uitgezonden, over ten minste twee ruimtelijke modi te verdelen. Bovendien moet de ononderscheidbaarheid van enkele fotonen van onze quantum dot één-foton bron gekarakteriseerd worden. Deze vragen worden behandeld in hoofdstukken 4 en 5.

In hoofdstuk 4 wordt de stroom van enkele fotonen probabilistisch verdeeld over twee paden met behulp van een Mach-Zehnder-interferometer (MZI) met een optisch padlengteverschil om fotonen die op verschillende tijdstippen zijn gecreëerd te laten interfereren. In dit hoofdstuk onderzoeken we niet alleen de ononderscheidbaarheid van onze bron van enkele fotonen, maar ook de correlaties die worden waargenomen bij een vertraging die overeenkomt met de interne vertraging van de interferometer. We geven zowel een intuïtieve verklaring voor de oorsprong van deze correlaties als een stelsel van vergelijkingen dat de correlaties bij alle mogelijke vertragingen beschrijft. Dit theoretische kader levert een uitdrukking op voor de ononderscheidbaarheid van enkele fotonen die rekening houdt met onevenwicht in de intensiteit van de twee paden in de MZI, en imperfecties in de voorbereiding van de polarisatietoestand van de fotonen. De validiteit van dit analytische model wordt geverifieerd aan de hand van experimentele gegevens die zijn verkregen door MZI's met zowel een korte (9 ns) als een lange (1 us) interne vertraging.

In hoofdstuk 5 onderzoeken we een meer deterministische verdeling van enkele fotonen over twee ruimtelijke modi met behulp van een optische switch. We geven een didactische uitleg van hoe demultiplexing de stroom van fotonen en de gemeten correlaties beïnvloedt. We stellen vast dat de normalisatie van de tweede-orde correlatiefunctie zorgvuldig moet worden uitgevoerd, vooral wanneer de schakeltijd slechts iets langer is dan het interval tussen opeenvolgende fotonen. Ten slotte presenteren we de gemeten correlaties voor onze gedemultiplexte quantum dot bron, waar de optische switch een schakeltijd van 1 us heeft. Hieruit blijkt dat bij langzame schakeling de normalisatiefout als verwaarloosbaar kan worden beschouwd.

In het laatste hoofdstuk van dit proefschrift integreren we de bevindingen uit de voorgaande hoofdstukken om tot een eerste experimentele demonstratie van quantum positieverficatie te komen. Voor deze demonstratie hebben we gekozen voor het twee-foton SWAP-protocol vanwege zijn volledige verliesbestendige eigenschappen. De resultaten tonen aan dat de Hong-Ou-Mandel (HOM) interferentiecontrast van onze één-foton bron de beperkende factor is, waardoor we de drempel niet kunnen bereiken om onderscheid te maken tussen een eerlijke bewijzer en tegenstander die opereren onder lokale operaties

en klassieke communicatie (LOCC). Modellering van de experimentele omstandigheden in combinatie met een state-of-the-art één-foton bron die in de literatuur wordt beschreven, geeft echter aan dat de LOCC-drempel binnen bereik ligt.

Verder onderzoek zou continue verbeteringen van hetzelfde protocol moeten bevatten met behulp van een state-of-the-art één foton bron. Eveneens is voortdurende ontwikkeling van QPV-protocollen van belang. Het doel is een protocol dat minimale quantum middelen vereist, de overdracht van quantum informatie met snelheden onder de lichtsnelheid mogelijk maakt, en volledig bestendig is tegen optische verliezen.

Curriculum Vitae

Kirsten Naomi Kanneworff

30-08-1996 Born in Zwijndrecht, the Netherlands.

Education

2008–2014 VWO Diploma, Dalton Lyceum Barendrecht, Barendrecht

2014–2017 Bachelor of Science in Physics
Universiteit Leiden
Thesis: The viability of single nucleotide detection using a graphene nanogap

2017–2020 Master of Science in Physics (cum laude)
Universiteit Leiden
Thesis: Electrical characterisation and critical behaviour of superconducting single photon detectors
Thesis: Towards experimental quantum position verification

2021–2026 PhD in Physics
Universiteit Leiden
Thesis: Experimental quantum position verification: practical challenges and single-photon correlations

List of publications

1. A. Bellunato, S. Vrbica, C. Sabater, E. W. de Vos, R. Fermin, **K. N. Kanneworff**, F. Galli, J. M. van Ruitenbeek and G. F. Schneider, Dynamic tunneling junctions at the atomic intersection of two twisted graphene edges, Nano Lett. 18, 4, 2505-2510 (2018).

2. **Kanneworff, K.**, Poortvliet, M., Bouwmeester, D., Allerstorfer, R., Lunel, P. V., Speelman, F., Buhrman, H., Steindl, P. & Löffler, W. Towards Experimental Demonstration of Quantum Position Verification Using Single Photons. Quantum Sci. Technol. 10, 045004 (2025).

Acknowledgements

First and foremost, I would like to thank **Wolfgang** for giving me the opportunity to pursue my PhD research in the group. Thank you for teaching me so much about what it means to be a scientist and for your continuous support throughout this journey. I am especially grateful for your understanding and encouragement during the more difficult times.

I spent the majority of my PhD working closely with **Petr** and **Matteo**, and I could not have wished for better colleagues. Petr, words cannot fully express how grateful I am for all the help you gave me, both in and outside the lab. Even after you moved to France for your postdoctoral position, you continued to meet with me online twice per week, which meant a great deal to me. Matteo, thank you for all the jokes and laughter that lightened the days, as well as for the serious check-ins when they were needed most.

Mio, your arrival in the group greatly boosted the progress I was able to make in the lab. I am particularly thankful for your dedicated work on the pulser, which ultimately made most of the results presented in this thesis possible.

Research is never done in isolation, and as part of my PhD training, I had the pleasure of supervising several bachelor's and master's students. **Killian** worked on understanding QPV through modelling. **Alicja**, **Camiel**, and **Hubertus** focused on polarization in optics. Alicja developed a model to predict outcomes after combinations of waveplates. Camiel measured the stability of polarization modulators and long optical fibres, as discussed in Chapter 3, and with Hubertus we investigated polarization mode dispersion, also discussed in that chapter. I am grateful to all of them for their contributions and enthusiasm.

I would like to thank **Harry** for setting up the research into QPV that formed the foundation of my PhD. I am also thankful for the collaboration with **Florian**, **René**, and **Philip**, which led to many interesting ideas and valuable theoretical support.

I am grateful to all past and present members of the quantum optics groups for the many lunches, drinks, and fun events we shared. In particular, I would like to thank **Thomas**, **Resi**, **Tom**, **Jacopo**, **Erik**, **Xing**, **Jonah**, **Corné**, **Xinrui**, **Leon**, **Hidde**, and **Felix** for the enjoyable time spent together. Over the years, many students have been part of the 9th floor, far too many to name. I would like to give a special thanks to **Ilse**, **Tessa**, **Yasmin**, and **Lisa** for becoming my friends and making the office a welcoming place. Furthermore, I would like to thank the quantum optics PIs **Dirk**, **Martin**, and **Michiel** for their guidance and for the many pleasant conversations, both scientific and otherwise, over the years.

I am thankful to **Henriette** for all the administrative support that helped keep everything running smoothly. **Kier**, thank you for all the clear explanations and patience in teaching me about the many different kinds of electronic circuits.

I would also like to thank the fine mechanics department (FMD) and the electronics department (ELD) for their invaluable help in building parts of the experimental setup. Beyond their technical expertise, I am grateful for the many enjoyable coffee moments,

which made working together a pleasure.

I would like to thank both **Sense-Jan** and **Jan** for giving me the freedom to explore the educational side of the PhD while working as your teaching assistant.

During part of my PhD, I was a member of the PhD platform. This would not have been possible without the support and help of **Koen** and **Solenn**, for which I am very grateful.

The PhD journey came with many ups and downs, and I would not have been able to get through it without my friends. **Bouke** and **Angelique**, I could always come to you to complain or talk things through when times were tough. **Job**, **Lars**, and **Floris**, you continually reminded me that there is always more to life than the time within the walls of the university. I would also like to thank the many friends I met during my time as a PhD candidate. In addition to the friends already mentioned throughout these acknowledgements, I want to thank **Amber**, **Peter**, **Norman**, **Maialen**, **Esra**, **Loek**, and **Guido**, who made this period all the more enjoyable.

My journey as a physicist would never have begun without the encouragement of my high school teacher **Jeroen Bruijstens**, who sparked my interest by allowing me to experiment freely with lab equipment.

Finally, none of this would have been possible without the love, care, and support of my family. I am deeply grateful to my parents and my brother for always believing in me.