Towards Experimental Quantum Position Verification

THESIS

submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE
in
PHYSICS

Author :	K.N. Kanneworff
Student ID :	s1520598
Supervisor :	Dr. W. Löffler
2^{nd} corrector :	Prof. Dr. H.M. Buhrman

Leiden, The Netherlands, November 8, 2020

Towards Experimental Quantum Position Verification

K.N. Kanneworff

Huygens-Kamerlingh Onnes Laboratory, Leiden University
P.O. Box 9500, 2300 RA Leiden, The Netherlands

November 8, 2020

Abstract

Authentication of a communication channel usually requires that the parties meet physically; but there is one solution if it is enough to confirm the geographical location of a party: quantum position verification (QPV). This is based on quantum mechanics, the no-cloning theorem, and special relativity, the invariance of the speed of light. We shown an extension of a QPV protocol where quantum information is communicated via the polarization state of single photons including the effects of photon loss and polarization noise, and explore it by numerical simulations. Moreover, we have designed and implemented the first steps of a QPV demonstration using optical fibers. We have been able to calibrate the setup for horizontal and vertical polarization states where a visibility of approximately 0.85 has been measured.

Contents

Chapter 1

Introduction

Nowadays almost all financial transactions are done via online banking. It would be helpful if we could verify that the bank's website webserver is located in the bank building in order to ensure safe communication. Safe communication requires (i) protection of the communication against eavesdroppers, and (ii) authentication of the identity of one party. The latter is much harder to achieve than the former, and usually requires either physical (going to a physical bank to do the transaction), or relying on a network of trust. Both are not ideal, the former is impractical and the latter is not fully secure.

Here we explore authentication of an, initially, untrusted party by geographic credential via position verification. Whether the third party can be trusted or not will depend on whether the party is at a claimed position or not. Quantum Position Verification (QPV) schemes in particular are a good candidate to safely use geographic credentials to authenticate a communication channel[1–3].

In the general one-dimensional Quantum Position Verification scheme there are three players. There are the two verifiers V_0 and V_1 and the

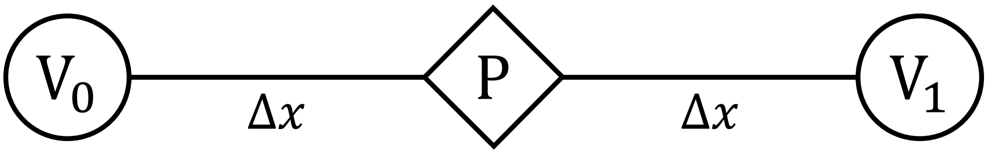


Figure 1.1: *General one-dimensional Quantum Position Verification scheme of the two verifiers V_0 and V_1 with the prover P exactly in between.*

prover P in the middle (fig 1.1). The goal of the quantum game is for the verifiers to check if the prover is exactly in the middle (at the agreed geographical position) or not. The two verifiers send out quantum information to the prover who in turn has to perform a task. The nature of the task depends on the protocol that is used. The result of the task is send back to both verifiers in the form of classical information. In the limit that all information travels at the speed of light, the time between the verifiers sending out the information and receiving the answer from the prover is 2Δx plus the time it takes for the prover to perform the task. If the prover is not in the position it claims (i.e. a dishonest prover) either the time for the verifiers to receive an answer for the prover is too long, or the results from the task do not follow the distribution of answers which would be

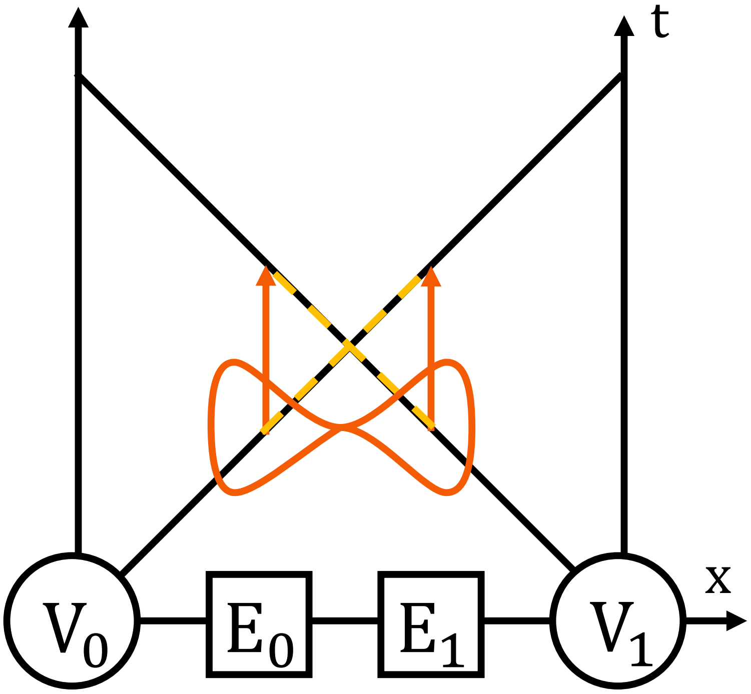


Figure 1.2: *Space-Time diagram of the scheme of two verifiers V_0 and V_1 with two eavesdroppers E_0 and E_1. The diagonal black lines is the space-time path travelled by the information. Each of the eavesdroppers intercepts the information from V_0 and V_1 after which they separately perform a task. The outcomes are communicated between the verifiers (yellow dashed line) and an answer for the verifiers is formulated by combining both results. There is a possibility that the eavesdroppers share entanglement (orange ∞), then the QPV scheme is broken.*

expected from an honest prover.

There is another possibility of an attack where an outside party tries to fool the verifiers into believing they are at the position of the prover P. We assume that this claimed position is not accessible to the malicious attackers, therefore an attacker can try to position two eavesdroppers E_0 and E_1 close to the location of the prover (figure 1.2). The space-time diagram shows that now eavesdropper E_0 is able to intercept some of all of the quantum information send by V_0 and the eavesdropper E_1 likewise for V_1. Both eavesdroppers can perform a task on the intercepted information. The eavesdroppers now also have the control over the classical channel over which they can communicate the results from their performed tasks (yellow dashed line in fig 1.2). Since the outcome of the task is in the form of classical information, the eavesdroppers are able to save a copy of the result as well (orange arrow). In the end, the eavesdroppers can formulate an answer to send back to the verifiers combining each others measurement outcomes. The goal of the attackers is now to emulate as good as possible the response of an honest prover.

These colluding adversaries (the eavesdroppers operating as a team) is the reason why the position verification schemes using classical information only break [4]. QPV has the verifiers use quantum information, limiting the attack possibilities for the eavesdroppers since the attackers are not able to copy the intercepted information anymore (no-cloning). However, it has been proven by Buhrman et al. [5] that it is possible for eavesdroppers to fool the verifiers when they (E_0 and E_1) share enough entanglement with each other. Hence, QPV is not safe against such attacks. Fortunately, it has later been shown by Beigi and Koenig [6] that the eavesdroppers need an exponential amount of EPR pairs (entangled states) and that QPV is still secure if only linear amounts of EPR pairs are available. Gaining an exponential amount of entanglement is very difficult, hence the protocols are secure for a large range of attacks.

This research is focused on moving Quantum Position Verification from theory to experiment by designing and setting up a demonstration of a QPV protocol. Here, we discuss a loss tolerant protocol and show the first calibration steps for an experimental one dimensional Quantum Position Verification demonstration. We first start with some background theory concerning polarization states of light and two path interference. In chapter 3 we discuss a QPV protocol proposed by Lim et al.[7] and explore the effects of loss and errors. In chapter 4 we design and discuss a first demonstration setup and show calibration results. At the end, in chapter 5, we discuss the found results and provide an outlook on further research.

Chapter 2

Background Theory

Before describing the protocol in more detail, a bit of background theory is necessary. This chapter provides a short overview on the topics of polarization states, waveplates, and the corresponding mathematics of Stokes parameters and Mueller matrices. Moreover, the protocol will use interferometry. In particular Hong-Ou-Mandel quantum interference of single photons and Mach-Zehnder interferometry.

Anyone with a Quantum Optics background will probably know the topics discussed in this chapter by heart and can skip it. The following chapters will refer back to the sections when necessary.

2.1 Bloch sphere and polarization states

Qubits are used to communicate information in the QPV protocol. In the research discussed here in this thesis, the polarization of single photons is used as a two-level system. Like any two-level system its state space can be represented by a Bloch Sphere (figure 2.1)[8]. Historically, the Bloch Sphere is known as the Poincare sphere in optics which was specifically designed for the polarization states[9].

The polarization of light is the direction in which the electric field oscillates. When light is linearly polarized, the electric field oscillates within a plane. Circular polarization is when the electric field circles around while a plane wave propagates.

In the case of quantum information the Bloch sphere has the computational basis $\{0,1\}$ on the north and south poles of the sphere. In the polarization mode the horizontal ($|H\rangle$) and vertical ($|V\rangle$) polarization states can, for instance, be considered the computational basis. On the surface of

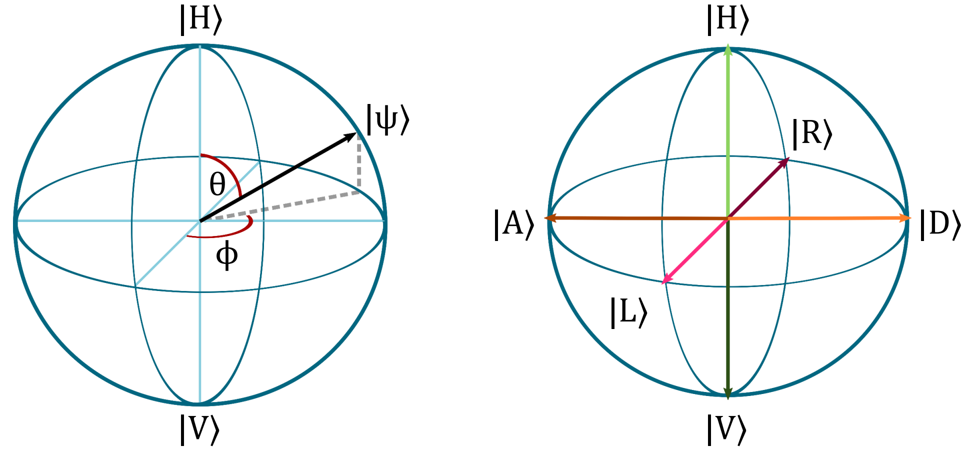


Figure 2.1: *Left: Pure state $|\Psi\rangle$ on the Bloch sphere with Bloch angles ϕ and θ. Right: Positions of the horizontal, vertical, diagonal, anti-diagonal, right circular and left circular polarizations.*

the Bloch sphere lie the pure states. Any pure polarization state $|\Psi\rangle$ can be defined as a function of two Bloch angles θ and ϕ, shown on the left in figure 2.1, in the following way:

$$|\Psi\rangle = \cos\left(\frac{\theta}{2}\right)|H\rangle + [\cos(\phi) + i\ \sin(\phi)]\sin\left(\frac{\theta}{2}\right)|V\rangle \tag{2.1}$$

Any state that lies inside the sphere is known as a mixed state, which is a statistical ensemble of pure states. These mixed states cannot be described as a vector like pure states. In this thesis we assume that all polarization states are pure states only.

In this thesis we focus use the six polarization states shown on the left in figure 2.1. The horizontal and vertical polarization states $|H\rangle$ and $|V\rangle$ form the computational basis and the two mutually unbiased bases (MUBs) to it: the Hadamard basis {+,-} and the {+i, -i} basis. In terms of polarization these bases are {D,A} (diagonal and anti-diagonal) and {R,L} (right and left circular polarized). The corresponding states from quantum information and in terms of polarization are shown in equation 2.2.

$$\begin{aligned}
&|0\rangle && |H\rangle \\
&|1\rangle && |V\rangle \\
&|+\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right) && |D\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle + |V\rangle\right) \\
&|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) && |A\rangle = \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle) \\
&|+i\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i\,|1\rangle) && |R\rangle = \frac{1}{\sqrt{2}}(|H\rangle + i\,|V\rangle) \\
&|-i\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i\,|1\rangle) && |L\rangle = \frac{1}{\sqrt{2}}(|H\rangle - i\,|V\rangle)
\end{aligned} \tag{2.2}$$

These six polarization states are all pure states. Therefore, they all can be described in terms of the Bloch angles θ and ϕ (eq 2.3).

$$\begin{aligned}
&|H\rangle : \theta = 0\,,\ \phi = 0 && |V\rangle : \theta = \pi\,,\ \phi = 0 \\
&|D\rangle : \theta = \frac{\pi}{2}\,,\ \phi = 0 && |A\rangle : \theta = \frac{\pi}{2}\,,\ \phi = \pi \\
&|R\rangle : \theta = \frac{\pi}{2}\,,\ \phi = \frac{\pi}{4} && |L\rangle : \theta = \frac{\pi}{2}\,,\ \phi = \frac{-\pi}{4}
\end{aligned} \tag{2.3}$$

As stated in the introduction, the protocol investigated in this thesis has the quantum information carried in the polarization state of single photons. In order for us to demonstrate the protocol we need to be able to prepare photons of different polarization which is done with waveplates.

2.2 Waveplates

Waveplates are free-space optical components made out of birefringent material and are used to alter the polarization state of the light travelling through it [10]. A birefringent material is optically anisotropic where the refractive index normal to the optical axis differs form the refractive index parallel to the optical axis. The parallel and normal axes are also known as the fast and slow axes. The difference in refractive index results in a phase difference between the components of the electric field which are parallel or normal to the optical axis.

The two most used linear retarders are the half-wave ($\lambda/2$) plate and the quarter-wave ($\lambda/4$) plate. The half-wave plate has a thickness such that the light travelling through experiences a relative phase shift of π in radians. When this plate is positioned at an angle τ w.r.t. the fast axis of the light, the electric field of linear polarized light exiting the plate has rotated over an angle 2τ. Hence, the half-wave plate rotates the direction of linear polarized light. Further, it inverts the handedness of circular polarized light.

The quarter-wave plate has a thickness such that the light through the plate experiences a relative phase shift of $\pi/2$ in radians. When linear polarized light travels through such a plate, oriented at 45° to an optical axis, it is rotated to circular polarized light and vise versa.

The results waveplates have on polarization states can be mathematically described with the use of Mueller matrices and Stokes parameters.

2.3 Mueller matrices and Stokes parameters

Stokes parameters are used to describe the polarization state of electromagnetic fields[11]. There are four stokes parameters which are linked to the intensity of the field for different polarizations (eq 2.4). S_0 is the total intensity, S_1 is the intensity difference between horizontal and vertical polarized light, S_2 is the difference between diagonal and anti-diagonal and, S_3 is the difference between right-handed and left-handed polarized light. For pure polarization states $\sqrt{S_1^2+S_2^2+S_3^2} = I$ where I is the total intensity measured.

$$\begin{pmatrix} S_0 \\ S_1 \\ S_2 \\ S_3 \end{pmatrix} = \begin{pmatrix} I_H + I_V \\ I_H - I_V \\ I_D - I_A \\ I_R - I_L \end{pmatrix} \tag{2.4}$$

From equation 2.4, one can define the six polarization states:

$$\begin{gathered}
|H\rangle = \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} \quad |V\rangle = \begin{pmatrix} 1 \\ -1 \\ 0 \\ 0 \end{pmatrix} \quad |D\rangle = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} \\
|A\rangle = \begin{pmatrix} 1 \\ 0 \\ -1 \\ 0 \end{pmatrix} \quad |R\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} \quad |L\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ -1 \end{pmatrix}
\end{gathered} \tag{2.5}$$

Any operation on these Stokes vectors are written as Mueller matrices [11], named after their developer Hans Mueller. In this thesis we use two types of Mueller matrices. The first one is the rotation matrix $R(\tau)$ with which the reference frame can be rotated from a local frame to the lab frame.

$$R(\tau) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \cos(2\tau) & \sin(2\tau) & 0 \\ 0 & -\sin(2\tau) & \cos(2\tau) & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{2.6}$$

The second type of Mueller matrix used is the operation performed by a linear retarder $M(\delta)$. The retardance (δ) is the phase difference induced between the field travelling along the fast and slow axes (as discussed in the section on waveplates). The operation of a linear retarder where the fast axis is set to 0° is given by equation 2.7[11].

$$M(\delta) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \cos(\delta) & \sin(\delta) \\ 0 & 0 & -\sin(\delta) & \cos(\delta) \end{pmatrix} \tag{2.7}$$

When the fast axis of the linear retarder is rotated by an angle τ w.r.t. the lab frame a combination of the rotation matrix and the matrix for a linear retarder is used to describe the change in polarization. First one rotates the reference frame to a local frame, then the operation of the retarder is applied after which the reference frame is rotated back to the lab frame. The Mueller matrix which describes this sequence of operations is given by equation 2.8.

$$R(\tau)M(\delta)R^{\dagger}(\tau) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \cos^2(2\tau)+\sin^2(2\tau)\cos(\delta) & \cos(2\tau)\sin(2\tau)(1-\cos(\delta)) & -\sin(2\tau)\sin(\delta) \\ 0 & \cos(2\tau)\sin(2\tau)(1-\cos(\delta)) & \sin^2(2\tau)+\cos^2(2\tau)\cos(\delta) & \cos(2\tau)\sin(\delta) \\ 0 & \sin(2\tau)\sin(\delta) & -\cos(2\tau)\sin(\delta) & \cos(\delta) \end{pmatrix} \tag{2.8}$$

For a half-wave plate and a quarter-wave plate the retardance is π, $\pi/2$ respectively. This means that for these two specific linear retarders the Mueller matrix is written as:

$$R(\tau)M(\pi)R^{\dagger}(\tau) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \cos^2(2\tau)-\sin^2(2\tau) & 2\cos(2\tau)\sin(2\tau) & 0 \\ 0 & 2\cos(2\tau)\sin(2\tau) & \sin^2(2\tau)-\cos^2(2\tau) & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \tag{2.9}$$

$$R(\tau)M\left(\frac{\pi}{2}\right)R^{\dagger}(\tau) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \cos^2(2\tau) & \cos(2\tau)\sin(2\tau) & -\sin(2\tau) \\ 0 & \cos(2\tau)\sin(2\tau) & \sin^2(2\tau) & \cos(2\tau) \\ 0 & \sin(2\tau) & -\cos(2\tau) & 0 \end{pmatrix} \tag{2.10}$$

2.4 Hong-Ou-Mandel interference

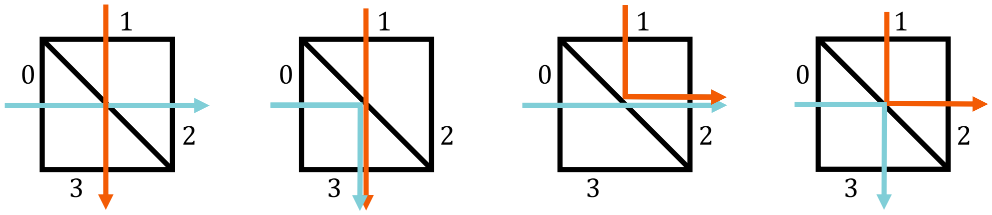
In the Quantum Position Verification protocol, that will be discussed in more detail in the next chapter, the prover performs a projection on a Bell-State. By performing this measurement the idea of quantum interference is used. Quantum interference between two single photons is also known as Hong-Ou-Mandel (HOM) interference[12].

This type of interference uses a 50:50 beam splitter where two photons arrive one each at the two inputs. The operation on the Fock (photon number) state is:

$$\begin{pmatrix} a_0^{\dagger} \\ a_1^{\dagger} \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix} \begin{pmatrix} a_2^{\dagger} \\ a_3^{\dagger} \end{pmatrix} \tag{2.11}$$

Where $a^{\dagger}$ is the creation operator for inputs 0 and 1 of the beam splitter and outputs 2 and 3. The multiplication with the imaginary number i, is a result of a $\pi/2$ phase change when the photon is reflected [13].

First there are two distinguishable (blue and orange) photons arriving at the beam splitter (figure 2.2). The blue photon arrives at input 0 (from the right) and the orange photon arrives at input 1 (from above). There are four possible outcomes: either both photons get transmitted, one is transmitted and the other reflected or both are reflected. Under the schematic representation of the four outcomes in figure 2.2 the mathematical expressions corresponding to the outcomes are written. Here $|1_b\rangle_2$ means that one blue coloured photon has ended up in output 2 of the beam splitter.

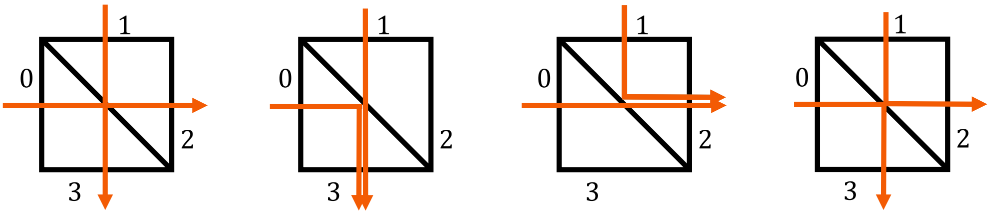


$$\frac{1}{2}|1_b\rangle_2\,|1_o\rangle_3 \quad + \quad \frac{i}{2}|0\rangle_2\,|1_b1_o\rangle_3 \quad + \quad \frac{i}{2}|1_b1_o\rangle_2\,|0\rangle_3 \quad - \quad \frac{1}{2}|1_o\rangle_2\,|1_b\rangle_3$$

Figure 2.2: *Schematic representation of the 4 possible outcomes of one blue photon and and one orange photon arriving at a 50:50 beam splitter. Below the mathematical expressions of the outcomes first in terms of the transmission and reflection coefficients and then the corresponding outcome for the 50:50 beam splitter (equation 2.11).*

The mathematical expressions of the outcomes where both photons are reflected and both photons are transmitted are different from each other. This logical, since the two photons have different colours.

Now, instead of a blue photon and an orange photon, both photons are orange. Providing that in every other mode (timing, polarization, orbital-angular momentum, etc) the two photons are exactly the same, they are completely indistinguishable (figure 2.3). In this case there is no way to tell if both photons are reflected or both photons are transmitted. Because



$$\frac{1}{2}|1\rangle_2\,|1\rangle_3 \quad + \quad \frac{1}{\sqrt{2}}|0\rangle_2\,|2\rangle_3 \quad + \quad \frac{1}{\sqrt{2}}|2\rangle_2\,|0\rangle_3 \quad - \quad \frac{1}{2}|1\rangle_2\,|1\rangle_3$$

Figure 2.3: *Schematic representation of the 4 possible outcomes of one orange photon arriving at each of the inputs of the 50:50 beam splitter. Below the mathematical expressions of the outcomes first in terms of the transmission and reflection coefficients and then the corresponding outcome for the 50:50 beam splitter (equation 2.11).*

the states are of opposite sign, the probability to generate an outcome where both outputs of the beam splitter receive one photon cancel each other out. As a result, both photons move to one of the two outputs of the beam splitter together. This phenomenon is Hong-Ou-Mandel interference. However, the cases of both transmitted or both reflected is only true when the two photons arriving at the beam splitter are completely indistinguishable in every way.

For Hong-Ou-Mandel interference we usually talk about single photons. The goal for this research is to build a demo experiment of QPV. We have not reached the point where we use single photons yet and used coherent light. Therefore, instead of Hong-Ou-Mandel interference we used a slightly different form of interference: Mach-Zehnder interference.

2.5 Mach-Zehnder interference and Visibility

The Mach-Zehnder interferometer (fig 2.4) is named after Ludwig Mach, who proposed the idea of such a device, and Ludwig Zehnder who refined the idea. In the Mach-Zehnder interferometer the light of a single source is send onto a beam splitter, splitting the light into two paths. The two paths are recombined at a second beam splitter. The interference pattern of the recombined light is then measured at one of the outputs[13][10].

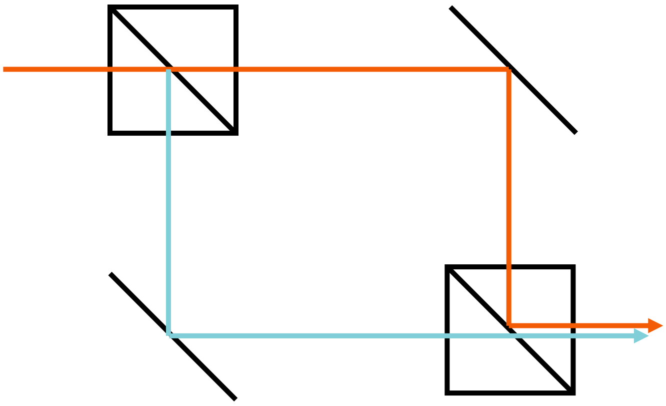


Figure 2.4: *Schematic representation of a Mach-Zehnder interferometer. The light of one source is split by the first beam splitter (upper left) into a transmitted beam (orange) and a reflected beam (blue). The two paths are recombined at a second beam splitter (lower right) and the resulting interference pattern is measured at one of the outputs.*

The interference pattern consists of interference fringes. The contrast of these interference fringes depends on how indistinguishable the light arriving at the second beam splitter is. Historically, the tuning of the indistinguishablity is performed by changing the path length of one of the arms. However, like mentioned in the previous section on HOM interference, the indistinguishablity also depends on other characteristics of light such as polarization.

The contrast of the interference fringes is known as interferometric visibility (or just visibility). The visibility $\mathcal{V}$ can be determined by measuring the maximum I_{max} and minimum I_{min} intensity values while changing the phase between the two paths (eq 2.12). If all other characteristics of the light are completely the same the maximum intensity must be the total intensity at the output and the minimum intensity should be zero. As a result the visibility should be 1. Any loss of overlap between the photon states in the two paths leads to a smaller value for the visbility[13].

$$\mathcal{V} = \frac{I_{max} - I_{min}}{I_{max} + I_{min}} \tag{2.12}$$

Chapter 3

Protocol and Simulations

The goal of Quantum Position Verification is to confirm if the prover P can be trusted by checking the geographic credentials. The space-time diagram of the studied one dimensional QPV scheme where two verifiers V_0 and V_1 confirm the position of prover P is shown in figure 3.1. Apart from assuming that the system is 1D, the assumption is made that the claimed position of the prover (the position that needs to be confirmed) is exactly between the two verifiers.

Like stated before in the introduction, the verifiers send quantum information to the prover who performs a set task. This nature of the quantum information and the task performed by the prover differ from protocol to protocol. The protocol discussed in this thesis has been proposed by Lim et al. where photons are used as single qubits [7]. This protocol is discussed in depth in this chapter. Moreover, we have performed simulations on this protocol to investigate the effects of error and loss are on the protocol and shortly discuss a small extension of the Lim protocol.

3.1 Lim Protocol

The QPV protocol proposed by Lim et al chooses photons as their single qubits. The quantum information in this scheme is stored in the polarization of the single photons send out by the verifiers. Here the prover makes use of a Bell-State Measurement to deduce whether the verifiers have send photons of equal or opposite polarization. A schematic of a Bell-State measurement with linear optics is shown on the right of figure 3.1. The photons from the verifiers arrive at a 50:50 beam splitter (BS) from paths 0 and 1. Depending on whether the photons are distinguishable or

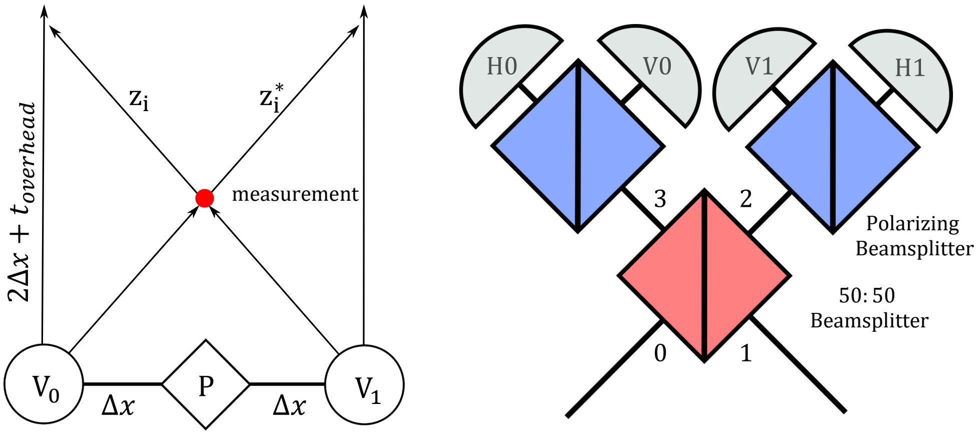


Figure 3.1: *Left: Verification scheme. Right: Bell-State measurement performed by honest prover. The photons arrive at paths 0 and 1 respectively and go through the 50:50 beam splitter (red) to the polarizing beam splitters where they are either transmitted or reflected which is detected by single photon detectors.*

not quantum Hong-Ou-Mandel interference happens.

After the first beam splitter the photons go through paths 2 and 3 to the polarizing beam splitters (PBS) where they are either transmitted or reflected to one of the two single photon detectors (H0, V0, H1, V1). It is important to note that only the polarization states from the Mutually Unbiased Bases (MUBs) from the measurement basis are used. In this protocol the measurement basis is {H,V}, meaning that the polarization state of the photons arriving at the PBS are split in their horizontal and vertical component. The MUBs from {H,V} are {D,A} and {R,L} which are therefore the only four polarization states used by the verifiers. When one of these four polarization states hits a PBS measuring in {H,V} the photon will either be reflected or transmitted with probability 1/2.

The Lim protocol, from choosing the polarization state to verification, can be divided into 5 steps: preparation phase, measurement by honest prover, eavesdropper check, quota check and verification.

1) Preparation phase: The verifier V_0 uses a random bit to determine the basis ({D,A} or {R,L}) and communicates the result with V_1 over a private channel. Then both verifiers take a random classical bit and from its result choose one of the two polarization states. The photons are sent to the prover at the same time, after the photons have been prepared in the chosen states.

2) Measurement by honest prover: When the photons arrive, the prover performs the Bell-State measurement (schematic drawn on the right in figure 3.1) and projects the incoming state onto one of the Bell-states. The measurement performed by the honest prover is a projection measurement on a Bell-state.

The photons arriving at the prover are of either equal or opposite polarization. In the case of equal polarization both photons either go into path 2 or path 3 due to HOM interference. As stated before, the PBS reflects or transmits an photon from one of the four possible states with probability 1/2. Therefore, there are three possible outcomes in this situation. Both photons are reflected and one V detector clicks, both photons are transmitted and one H detector clicks or one photon is transmitted and the other reflected and both single photon detectors on the same side click. The last outcome gives a coincidence count and shows that both photons had arrived at the prover. For this result, we assign $z = 0$. The first two outcomes only give one detection event which, assuming the detectors used are not photon number resolved, cannot be distinguished from a situation where one of the two photons was lost before arriving at the prover. Because no information can be gathered from such a detection event, this result is considered inconclusive ($z = ø$).

When the incoming photons are of opposite polarization, no interference takes place at the 50:50 BS. Here there is the possibility for one photon to be directed into path 2 and the other into path 3. When this happens the H detector on one side and the V detector on the other side click. For this detection event, we assign $z = 1$. When both photons are directed into the same path only one detector will click and is considered an inconclusive result with $z = ø$.

The honest prover sends the result back to the verifiers over a classical channel where the information travels with the speed of light.

3) The eavesdropper check: When the verifiers receive the result from the honest prover they check two things. The first is the timing of the result. The time between the verifiers sending the quantum information and receiving the classical information is two times the distance plus an overhead time (space-time diagram figure 3.1). The time it takes for the prover to perform the Bell-State measurement is included into this overhead time. The other requirement is that both verifiers must receive the same answer from the prover. If either one of these conditions is not met, there is a high probability that eavesdroppers are present and the verifiers abort the protocol immediately. If both conditions are met, the verifiers continue and prepare another photon state to send. The first three steps of the protocol are repeated m times.

4) The quota check: The verifiers count the amount of conclusive results sent back by the prover after all m iterations are received. This sum s must be larger or equal to a set threshold n_{th}. This threshold is set to half of the iterations, since the probability an honest prover measures an conclusive result is $\frac{1}{2}$. If the number of received conclusive answers is smaller than the set threshold, the protocol is seen as not successful and is aborted.

5) Verification: All inconclusive results are discarded and a random subset of size n_{th} is taken. The verifier V_1 communicates his set of random classical bit values, which determined the polarization state of the photons on his side, with the verifier V_0 over the private channel. V_0 then uses the information to count the instances when the received answer is incorrect (r). Verification is considered successful when:

$$\delta = \frac{r}{s} \leq \delta_{th} = 1 - P_{max}^{LOCC} \tag{3.1}$$

Where P_{max}^{LOCC} is the maximum guessing probability of LOCC attackers which is 3/4. The LOCC attackers are explained in more detail in section 3.1.1. Hence, the amount of incorrect answers divided by the amount of conclusive answers must be smaller or equal to 1/4.

3.1.1 LOCC attackers

There is a possibility that there is no prover, but there are attackers who want to fool the verifiers into believing that they are in the middle (the claimed position). In order for the attackers to receive all the information communicated with the prover, there has to be an attacker for every verifier in the scheme. One group of attackers are LOCC attackers who have access to a subset of generalized quantum measurements known as local operation and classical communication (LOCC)[14]. Here in this thesis we assume that all attackers fall into this group.

An attack the LOCC can perform is that both eavesdroppers try to measure the polarization state of the incoming photon and communicate the results with each other. With the classical information shared between the eavesdroppers they both send an answer back to the verifiers (for a space-time diagram including the eavesdroppers see figure 1.2) Since the photons are prepared by the verifiers in one of the two bases, the eavesdroppers can guess the correct bases to measure in with probability $\frac{1}{2}$. If the correct basis is chosen, the measured result will always be correct. If the attackers have chosen the wrong basis, they can guess the correct result with probability $\frac{1}{2}$. Therefore the maximum guessing probability of the LOCC attackers is:

$$P_{max}^{LOCC} = \frac{1}{2}\left(1 + \frac{1}{2}\right) = \frac{3}{4} \tag{3.2}$$

The error made by the attackers is 1/4 (1 minus the guessing probability) and as a result the error made by any honest prover must be smaller than this value.

3.2 Simulation

We have done simulation in order to estimate the success probability of the protocol under varying conditions. In the simulation we made two assumptions: the polarization of the photons is always a pure state and the eavesdropper check is ignored, i.e. the classical information from the prover are always within the set time and both verifiers always receive the same information. As a result of the first assumption, the polarization states are defined as:

$$\begin{aligned} |\Psi\rangle &= \cos\left(\frac{\theta}{2}\right)|H\rangle + [\cos(\phi) + i\ \sin(\phi)]\sin\left(\frac{\theta}{2}\right)|V\rangle \\ |\Phi\rangle &= \cos\left(\frac{\theta}{2}\right)|H\rangle + [\cos(\omega) + i\ \sin(\omega)]\sin\left(\frac{\theta}{2}\right)|V\rangle \end{aligned} \tag{3.3}$$

The combination of the basis choice and outcome of the random classical bit determine the Bloch sphere angles in equation 3.3.

To simulate the measurement by the honest prover, the probabilities for the three possible outcomes ($z = 0$, $z = 1$ and $z = ø$) were determined as a function of the Bloch angles. In order to make this derivation a bit more comprehensible equation 3.3 is simplified to:

$$\begin{aligned} |\Psi\rangle &= a|H\rangle + b|V\rangle \\ |\Phi\rangle &= u|H\rangle + v|V\rangle \end{aligned} \tag{3.4}$$

Where $a, b, u, v \in \mathbb{C}$. Then, using a combination of the transformation matrix of a 50:50 beamsplitter and the density matrix formalism, the probabilities for the three measurement outcomes are defined as:

$$\begin{aligned} P_0 &= \frac{1}{2}\left[|a|^2|v|^2 + ab^*u^*v + a^*buv^* + |b|^2|u|^2\right] \\ P_1 &= \frac{1}{2}\left[|a|^2|v|^2 - ab^*u^*v - a^*buv^* + |b|^2|u|^2\right] \\ P_ø &= \frac{1}{2}\left[2|a|^2|u|^2 + 2|b|^2|v|^2\right] \end{aligned} \tag{3.5}$$

Where a^* is the complex conjugate of a and $|a|^2 = aa^*$. The full derivation of the outcome probabilities is found in appendix A. All together the outcomes correspond to the calculated probabilities. In the ideal situation, half of this list is the correct conclusive outcome and the other half are inconclusive results. After the creation of the list, one outcome/one element of the list is chosen randomly and is the result which the prover sends back.

The Lim protocol assumes ideal conditions, i.e. all prepared polarization states are exactly as intended and remain unchanged during transport from the verifier to the prover and that the photons are not lost in the quantum channel. However, in an experiment neither assumption, our simulation considers errors in the polarization state and loss.

3.2.1 Non-ideal polarization states

In the experiment there is a probability that the polarization of the photons send by the verifiers are changed in their polarization state before arriving at the prover. These changes in polarization state can lead to the prover sending back an incorrect answer, hence increasing the error rate.

In order to quantify this error we have defined an error coefficient R. If $R = 0$ there is no error and the photons are in the expected polarization state. If $R = 1$ the input received by the prover would be the exact opposite of what was intended by the verifiers. For example, if the verifiers would want to send two photons of equal polarization, the prover would receive two photons of opposite polarization. As a result the honest prover would only send back the result $z = 1$ instead of the expected $z = 0$.

In short, a change in R leads to a shift in the probabilities to measure one of the two conclusive results ($z = 0$ or $z = 1$). In the case of equal polarization the probability to measure the correct answer is $P_0 = 1/2$ when there is no error. If the error is maximum, the probability to measure the correct answer is zero. Therefore, in the case of equal polarization the relation between R and P_0 is:

$$P_{i=0} = \frac{1}{2}(1 - R) \tag{3.6}$$

As shown in equation 3.5, these probabilities are depending on the Bloch sphere angles of the two states. The error in the polarization state can be visualized by adding two Bloch angles γ and ϵ and change the expression of $|\Phi\rangle$ in equation 3.3 to:

$$|\Phi\rangle = \cos\left(\frac{\theta+\gamma}{2}\right)|H\rangle + (\cos(\omega+\epsilon) + i\ \sin(\omega+\epsilon))\sin\left(\frac{\theta+\gamma}{2}\right)|V\rangle \tag{3.7}$$

Here γ and ϵ are corrections on the expected Bloch angles θ and ω. We assume that one of the two verifiers only produces the intended polarization state. Hence, the expression of $|\Psi\rangle$ remains unchanged and the angles γ and ϵ are the relative phase between the states $|\Psi\rangle$ and $|\Phi\rangle$.

A relation between the Bloch angles and the error coefficient is found by putting equation 3.7 into the expression of P_0 (eq: 3.5). And solve for the case of equal polarization state (eq: 3.6). The result of the derivation is given by equation 3.8. A full derivation of this expression is given in appendix B.

$$\cos(\gamma)\cos(\epsilon) = 1 - 2R \tag{3.8}$$

This relation is the same when one would look at the case of opposite polarization. The expression is also symmetric for both γ and ϵ and therefore only define the error through changing γ while keeping $\epsilon = 0$.

3.2.2 Loss of photons

In experiments there is a high probability that a single photon is lost somewhere. The probability that a photon send by the verifier is received by the prover is given by the transmission coefficient η. If one of the two photons is lost, the honest prover will only measure one detection event and the result will be considered inconclusive. When both photons are lost, the prover measures nothing and this is also considered an inconclusive result. The probability that one photon is lost and the other transmitted is $2\eta(1-\eta)$. The probability that both photons are lost is $(1-\eta)^2$.

If $\eta = 1$, the honest prover only measures an inconclusive result with probability $1/2$ due to the nature of the projection measurement. If $\eta = 0$, no photons arrive at the position of the prover and the prover measures only inconclusive results.Taking this into account, the probability of measuring an inconclusive result as a function of the transmission coefficient is given by equation 3.9. Here $P_ø$ is the probability of an inconclusive answer as defined in equation 3.5.

$$\tilde{P}_ø(\eta) = P_ø\left[1 + 2\eta\,(1-\eta) + (1-\eta)^2\right] \tag{3.9}$$

$$\tilde{P}_{i=0,1}(\eta) = P_{i=0,1}\cdot\eta^2 \tag{3.10}$$

Similarly the probability to measure $z = 0$ or $z = 1$ as a function of transmission is given by equation 3.10. Here $P_{i=0,1}$ is the probability P_0 or P_1 as function of polarization given by equation 3.5.

The inclusion of photon loss also leads to a need to redefine the threshold set for the the quota check (n_{th}). In the Lim protocol this is set to half of the iterations, but with loss of photons this threshold cannot be reached. Therefore, the threshold must also be depending on the transmission coefficient.

$$n_{th}(\eta) = \left(1 - \tilde{P}_{\o}(\eta)\right) \cdot m = \frac{1}{2}\eta^2 \cdot m \tag{3.11}$$

3.2.3 Simulation results

By using the formalism for the polarization error and photon loss we have simulated the success rate of the protocol as a function of both effects. Like in the protocol, the creation of the state and the measurement by the prover are repeated m times. Only here we assumed that both verifiers receive the answer from the prover in time and both receive the same answer, therefore always succeeding the eavesdropper check. Then the quota check and verification steps are performed as described in the protocol. The whole protocol is repeated 9 more times and the success rate is determined by averaging over these 10 attempts.

Figure 3.2.a shows the result of the simulation. Here the success rate of the protocol (the average of running the protocol 10 times) is plotted as a function of both the transmission η and the error R. The protocol run in this simulation was 500 iterations long and the quota threshold n_{th} was set as a function of transmission (eq 3.11). The black line drawn is the boundary where $R = 1/4$. This is the maximum error for which the honest prover can be distinguished from a dishonest one.

The region where η is close to zero and the success rate of the protocol is zero, is an artefact from the simulation. The calculated value of n_{th} in this region becomes smaller than 1. In the simulation any value smaller than 1 would be considered 0 and the protocol would always be a success. This would also be an artefact and choosing the lesser of two evils, we have set the protocol to fail if the value of $n_{th} < 1$.

For a high transmission there is some spread in success rate of the protocol as function of the error coefficient. This spread increases when the photon loss increases. The divergence in success rate for lower transmission is a direct result of how the verification check is defined in the protocol (eq 3.1). The amount of incorrect answers r can be approximated as the probability of an incorrect answer multiplied n_{th}, the size of the random subset. In other words $r \approx Rn_{th}$, since a subset of size n_{th} is taken from the set of conclusive results. The amount of conclusive results s depends on the amount of iterations and the transmission coefficient in the same way as n_{th}, hence $s \approx n_{th}$. In conclusion, equation 3.1 can be approximated as:

$$\frac{r}{s} \approx \frac{Rn_{th}}{n_{th}} = R \leq \frac{1}{4} \tag{3.12}$$

The quota check succeeds when the amount of conclusive answers is equal to or larger than the set threshold n_{th}. Therefore, there is a possibility that $s > n_{th}$. To take this into account we define $s = n_{th} + \Delta$ where Δ is the number of answers with which the amount of conclusive answers exceeds the threshold. Now equation 3.1 should be rewritten as:

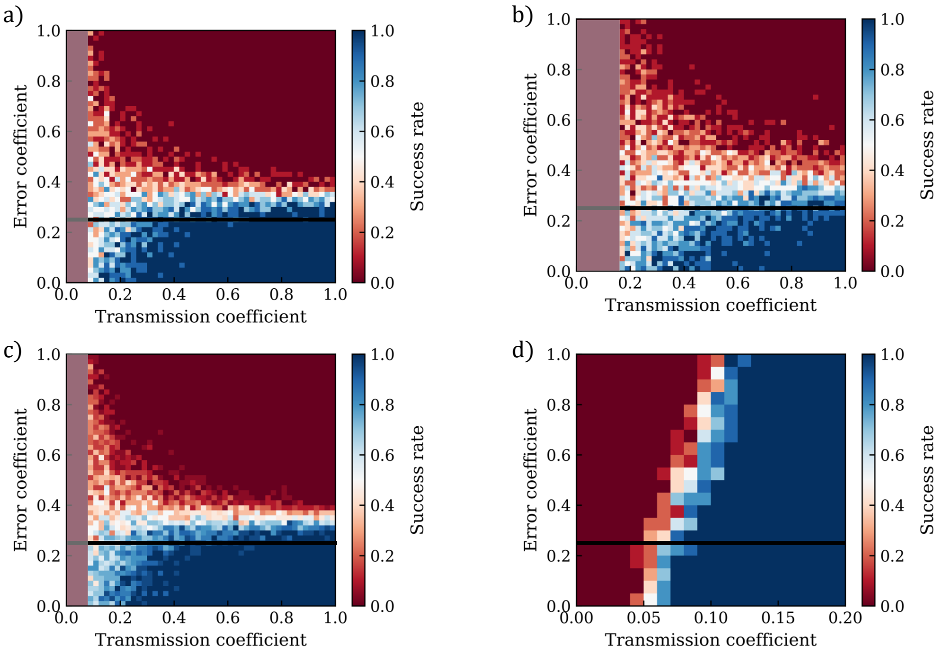


Figure 3.2: *Success rate of the Lim protocol as a function of R and η. The black line is where $R = \frac{1}{4}$, the limit in error for an honest prover. a) n_{th} follows equation 3.11, $m = 500$, rate is averaged over 10 repetitions. b) similar to a, but $m = 100$. c) similar to a, but rate is averaged over 20 repetitions. d) $n_{th} = 10$, $m = 5000$, rate is averaged over 10 repetitions. The grey-red areas on the left in a-c is where $n_{th} = 0$ and the simulation stops functioning.*

$$\frac{r}{s} \approx \frac{Rn_{th}}{n_{th}+\Delta} \leq \frac{1}{4} \rightarrow R \leq \frac{1}{4}\left(1+\frac{\Delta}{n_{th}}\right) \tag{3.13}$$

Here Δ is a small number and when the transmission is high $n_{th} >> \Delta$. In this case the error coefficient for which the protocol might still give a success to the protocol is close to $1/4$. However, when the transmission decreases, and the amount of iterations done in the protocol remains the same, n_{th} decreases as well. The limit $n_{th} \approx \Delta$ is reached for sufficiently low η. As a result, the boundary for R is set to $1/4$, increases with decreasing n_{th} and the protocol has a possibility to be successful even if the error is much larger than $1/4$.

The cause of the spread can be shown more clearly by doing the same simulation, but going through less iterations than before. The result of this simulation is shown in figure 3.2.b where everything is equal to the simulation in a, but the amount of iterations has been decreased from 500 to 100. The value of n_{th} in this new simulation is also 5 times smaller. By reducing the number of iterations, the impact of a nonzero Δ increases and the spread of success rate as function of R is larger even for full transmission. The zero success rate region on the left of the figure is larger, because n_{th} becomes smaller than 1 for a higher transmission.

The success rate in the simulation is determined by repeating the protocol ten times for each combination of η and R. Therefore, the success rate plotted is not absolute and the result of the simulation can have small deviations between runs. In order to check if the amount of repetitions over which the result is averaged leads to artefacts, we performed the same simulation as for figure 3.2.a, but the amount of repetitions is increased from 10 to 20. The result of the simulation is shown in figure 3.2.c. Comparing the two graphs shows that the shape and size of the features are comparable and are only a bit more blurred with the increased repetitions.

When performing the experiment, the transmission of the quantum channels should be determined before the protocol is started. For this transmission, the number of iterations m should also be chosen. This leads to a fixed value of n_{th}. We performed the simulation for a fixed threshold $n_{th} = 10$ and number of iterations $m = 5000$. This simulation is done over a smaller range in η and the outcome is shown in figure 3.2.d.

In this case the verifiers assume that the quantum channels used have a transmission of approximately 6%. The simulation shows that when the actual transmission is larger than the expected value, the protocol can give a successful verdict even though the error is larger than the set value of $1/4$. This is again caused by the verification check. Again we do the approximations that $r \approx Rn_{th}$ and $s \approx \frac{1}{2}\eta^2 m$. Then substituting this into equation 3.1 and filling in $n_{th} = 10$ and $m = 5000$ leads to:

$$\frac{r}{s} = \frac{Rn_{th}}{\frac{1}{2}\eta^2 m} = \frac{10R}{2500\eta^2} \leq \frac{1}{4} \tag{3.14}$$

For an honest prover R cannot be larger than 1/4, otherwise one cannot make the distinction between the honest and dishonest prover. As a result $n_{th}/\frac{1}{2}\eta^2 m$ should not be differ much from 1.

In conclusion, we have looked at the success rate as a function of both the photon loss and the polarization error. Both factors lead to a change in the answer distribution expected for an honest party. The loss of photons results in a higher probability of an inconclusive answer than expected in the Lim protocol. The polarization error leads to the probability of the prover answering incorrectly. This is not expected in the theoretical case described in the Lim protocol where the prover only gives back a conclusive and correct answer or an inconclusive answer.

From the simulations we see that the limiting factor is the transmission of the quantum channels. If the set threshold for conclusive results received is too low or when the transmission coefficient fluctuates too much, it is possible for the protocol to succeed even if the error exceeds the set 1/4. In this case, there the verifiers will not be able to distinguish between an honest and dishonest prover. In order to set a high enough threshold for the quota check (n_{th}) at high photon loss, the protocol must go through many iterations and the protocol will take a longer time. And if necessary, the transmission of the channel needs to be stabilized.

3.3 Slight extension of the Lim protocol

In the Lim protocol the verifiers are able to choose between the bases {D,A} and {R,L}. But what if the verifiers were also allowed to choos the third Mutually Unbiased Basis {H,V}?

In this case any LOCC has to choose between three different bases, and can only do so with probability 1/3. In the case they choose the correct basis, they can return the correct answer with probability 1 like before. However, now there are two possible situations where they choose the incorrect basis in which case they can only guess the correct result with probability 1/2. Therefore, the maximum guessing probability would change into:

$$P_{max}^{LOCC} = \frac{1}{3}\left(1 + \frac{1}{2} + \frac{1}{2}\right) = \frac{2}{3} \tag{3.15}$$

Apart from a lower guessing probability, adding the {H,V} basis provides an extra measure to detect any presence between the verifiers and the honest prover. When the honest prover receives two photons with equal polarization and polarized in the same basis in which the result is measured (in this case the {H,V} basis) only one detection event takes place. For example, both verifiers produce an H-polarized photon and send it to the prover. Due to HOM-interference both photons go into one of the two paths together and are both transmitted through the polarizing beamsplitter resulting in an inconclusive outcome. Contrary to the photons of equal polarization form one of the other two bases the probability of measuring a conclusive result is zero (assuming there is no error).

So in the case where there are eavesdroppers present, there is a possible situation where the verifiers receive a conclusive answer while sending out either H-polarized or V-polarized photons. Upon receiving such an answer the verifiers will afterwards know that a third party was present and can declare the verification to be unsuccessful.

Chapter 4

Experimental setup

In the previous chapter we discussed the proposed Lim QPV protocol and performed simulation to explore it. Now we move from theory to experiment. In this chapter we show the first demonstration setup for Quantum Position Verification. This setup uses fiber based polarization controllers which are discussed in more depth. After discussing the calibration process for the polarization states send out by the verifiers, the results of this calibration are shown.

4.1 Setup

The setup can be divided into two sections: the verifiers and the prover. For the verifiers it is important that they are able to change the polarization state at will. The prover performs a Bell-State Measurement (BSM) discussed in the previous chapter.

The research presented in this paper is a step towards a demo experiment of QPV and does not operate with single photons yet, for now a coherent light source (laser) is used. Moreover, in this project we use optical fibers instead of performing the experiment in free space. The reason for this decision is that in fibers, photons are able to travel over large distances without it taking up much space. However, the ″problem″ with using optical fibers instead of free space is that the maximum velocity through a fiber is 2/3 the speed of light. Consequently, this setup does not comply with the relativistic constraint set in QPV.

A schematic representation of the build setup is shown in figure 4.1. The setup starts with a combination of the laser ($\lambda = 830$ nm) and a polarizer placed in free space. This polarizer is used to be sure that all photons

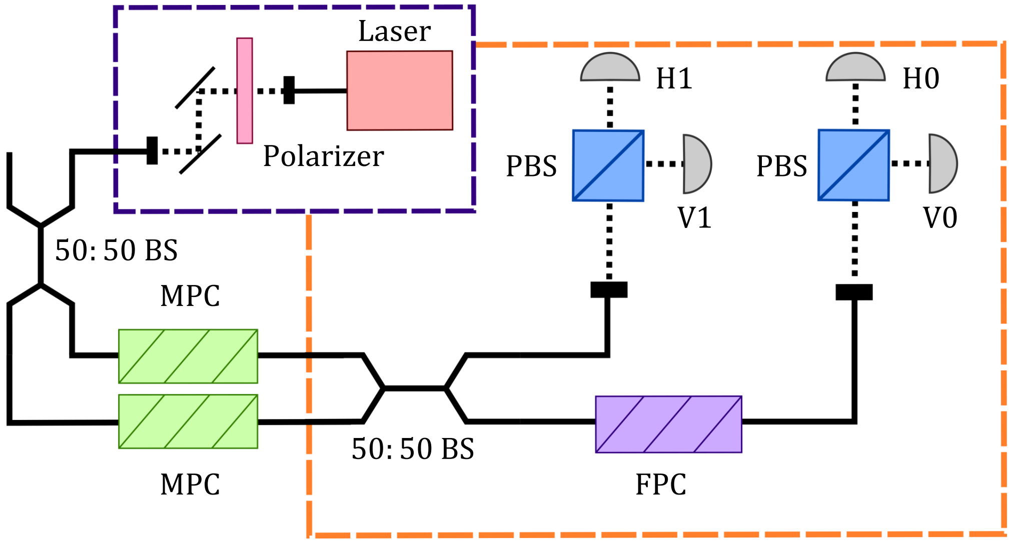


***Figure 4.1:** Schematic representation of the build fiber based QPV demonstration setup. The setup consists of a coherent light source (purple box), two verifiers represented by the motorized polarization controllers (MPC) and the Bell-state measurement performed by the prover (inside orange dashed box) with an additional fiber based manual polarization controller (FPC).*

are of the same polarization in the beginning. This part of the setup will be removed when using either a SPDC (Spontaneous Parametric Down Conversion) or quantum dots as single photon source, since all photons from these sources have the same polarization state.

For simplicity, we only use one light source for both verifiers, therefore the light is split into two paths by a 50:50 fibersplitter after the light was coupled into a single-mode fiber. The two light beams are sent to the verifiers who are represented by Motorized Polarization Controllers (MPC). These MPCs are fabricated by Thorlabs (Thorlabs MPC320) and use a combination of bending and twisting of the single-mode fiber to alter the polarization state of the light. The next section of this chapter provides a more in-depth examination of these MPCs.

Like in the original protocol, after the verifiers have altered the polarization state of the light, the information is send to the prover who performs a probabilistic BSM. The full BSM is framed by the orange dashed line. It starts with another 50:50 fibersplitter (Thorlabs TW850R5A2) where, depending if the incoming light is of equal or opposite polarization, HOM interference takes place. After the fibersplitter, the photons are coupled out of the single-mode fibers and travel towards the two free-space polarizing beamsplitters (Thorlabs PBS202). At the outputs of the PBS, the light is coupled back into multi-mode fibers which are attached to photodiodes (Thorlabs TW850R5A2). We used these photodiodes instead of single-photon detectors, since we used a coherent light source. In one of the two outputs of the fibersplitter there is a manual Fiber Polarization Controller (FPC) from Thorlabs (Thorlabs FPC560). The single-mode fibers after the second fibersplitter alter the polarization state of the photons travelling through it. The FPC is there to make sure that the change in polarization state is equal in both paths.

4.2 Fiber Polarization Controller

In the setup we used fiber based polarization controllers, which are either motorized (MPC) or manually driven (FPC). These devices consist of three paddles which can rotate independently from each other. A single-mode fiber is threaded through the device where it is bend in loops around each paddle. The combination of the loops made in the single-mode fiber and the twisting of the fiber due to the rotation of the paddles create stress-induced birefringence in the fiber. The birefringence alters the polarization state of the incoming light like waveplates which are made of birefringent materials. Therefore, these devices are used for the verifiers to continuously switch between polarization states as is needed in the protocol.

In this section we will briefly discuss stress-induced birefringence and show that the three paddles of these fiber based polarization controllers act similar to a sequence of waveplates: $\lambda/4$, $\lambda/2$ and $\lambda/4$ which can be rotated independent from each other.

4.2.1 Stress-induced birefringence

The stress-induced birefringence in a single-mode fiber is caused by bending and twisting of the fiber. Bending a single-mode optical fiber into loops leads to a result comparable with the effect of a linear retarder with retardance δ [15]. The retardance created for one paddle depends on several properties of both the light and the fiber used. This dependence is shown in equation 4.1, where δ is the retardance in radians, a is the fiber photo-elastic coefficient (0.133 for silica fiber) [16], N is the number of loops, d is the fiber cladding diameter, λ is the wavelength of the light and D is the diameter of the loops.

$$\delta(\text{radians}) = 2\pi^2 a \; N \, \frac{d^2}{\lambda D} \tag{4.1}$$

The type of single-mode fibers used are 780-HP fibers from Thorlabs. From this we know that the fiber cladding diameter is $d = 125 \pm 1\mu$m. Furthermore, we know that the paddles have a diameter of 18mm and that the wavelength of the laser is $\lambda = 830$nm. The goal is to create two $\lambda/4$ plates with one $\lambda/2$ plate in between. The number of loops always needs to be an integer value for obvious reasons. For an approximation of a $\lambda/2$ plate $N = 1$ and for a $\lambda/4$ plate $N = 3$. With this information the expected retardance for both a $\lambda/2$ plate (δ_2) and for a $\lambda/4$ plate (δ_4) were calculated.

$$\delta_2 = 2\pi^2 \, \frac{0.133 * 1 * (125\mu m)^2}{826nm * 18mm} \approx 0.88\pi \tag{4.2a}$$

$$\delta_4 = 2\pi^2 \, \frac{0.133 * 3 * (125\mu m)^2}{826nm * 18mm} \approx 2.63\pi \tag{4.2b}$$

Rotating the MPC paddles results in the twisting of the single-mode fiber [17, 18]. This rotation creates a local reference frame with an angle τ w.r.t. the lab reference frame. As a result there is a rotation of 2τ of the fast axis of the polarization before and after the paddle. This rotation is also known as the geometrical contribution of the birefringence axis. There is a slight difference between the angle τ during the experiment and in the theory when using the MPC. The MPC can only move between 0° and 170°, but they have defined to have the fast axis of the fiber aligned with the loops when the angle made by the MPC is 85°. This means that the angle with which the birefingence axis is rotated corresponds to the rotation angle of the MPC paddle (we will call τ_{lab}) as $\tau = \tau_{lab} - 85°$.

There is a second contribution known as the photoelastic contribution. A twist of the fiber with angle τ leads to a rotation of the polarization state with angle θ. The relation between the angles τ and θ is given by equation 4.3 where α is a constant depending on the refractive index n and elasto-optical coefficient p_{44}.

$$\theta = \alpha\tau; \alpha = -n^2 p_{44} \tag{4.3}$$

There are several values found in literature for α. Ulrich et al. [17] say that $\alpha = 0.16$ and Tentori et al. [18] calculated a value of $\alpha = 0.92$. This contribution is not taken into account in the following section, since the elasto-optical coefficient for single-mode fibers we used has to be determined experimentally.

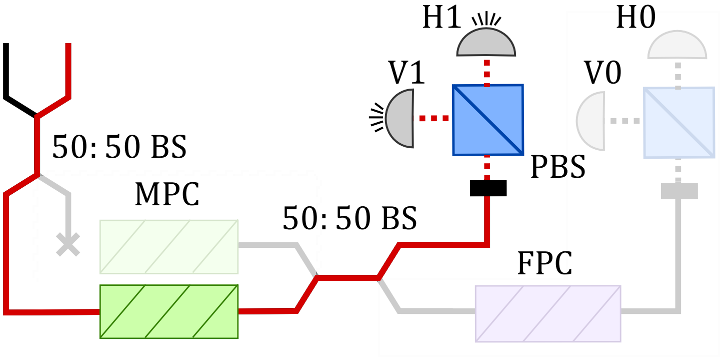


Figure 4.2: *The first step in the calibration process where only one of the two Motorized fiber Polarization controllers is attached. The intensity of the light is measured at the outputs H1 and V1 of the Polarizing Beam Splitter while the three paddles of the MPC are rotated.*

The combination of the retardance from bending the single-mode fiber and the geometric contribution from twisting the fiber is comparable to the effect waveplates have on the incoming polarization state. Therefore, we represent each paddle with the Mueller matrix from equation 2.8. It is possible for each paddle to have a different value of τ and the first and third paddle have a different retardance than the second paddle. Hence the full MPC is given by the following combination of matrices:

$$M_{MPC} = R(\tau_1)M(\delta_4)R^{\dagger}(\tau_1)R(\tau_2)M(\delta_2)R^{\dagger}(\tau_2)R(\tau_3)M(\delta_4)R^{\dagger}(\tau_3) \quad (4.4)$$

The output of the MPC for certain settings can be modeled when the input Stokes vector is known via the relation $\vec{S}_{out} = M_{MPC}\vec{S}_{in}$.

4.2.2 MPC measurements

The first step in the calibration process of the demo-experiment is the calibration of one of the two MPCs. Figure 4.2 shows a schematic representation of this step. The intensity of the light are detected at positions H1 and V1 behind the PBS while the three paddles of the MPC are rotated. The first (τ_1) and third (τ_3) paddle are moved from 0° to 170° in increments of 10°. For each combination of τ_1 and τ_3, the second paddle (τ_2) is rotated over the full range in 5° increments.

The intensity of the light as function of τ_2 for a fixed combination of τ_1 and τ_3 is displayed by the circles in figure 4.3. First the measurement was performed for the horizontal polarized output of the PBS (blue circles). Then the measurement was performed again for the vertical polarized input of the PBS (orange circles). The intensity was measured with the use of a Thorlabs PM100D. The average sum over both outputs was calculated ($I_0 \approx 212\mu$W) over which the measured intensities were normalized. Since τ_1 and τ_3 are kept constant, this data displays the effect of rotating a $\lambda/2$ plate for a unknown input polarization.

From the measured intensities of the H and V polarization we calculated the values the Stokes parameters S_0 and S_1. From equation 2.4 we know that S_0 is the sum of the intensities measured at H1 and V1, while S_1 is the difference. The other two Stokes parameters S_2 and S_3 cannot be extracted from the data, since these are only dependent on the intensity of diagonal or circular polarized light and we have only measured in the {H,V} basis. These calculated values were also normalized over the average sum of both outputs. S_0 is quite constant meaning that the laser remains constant over the time one of these measurements take which is several minutes.

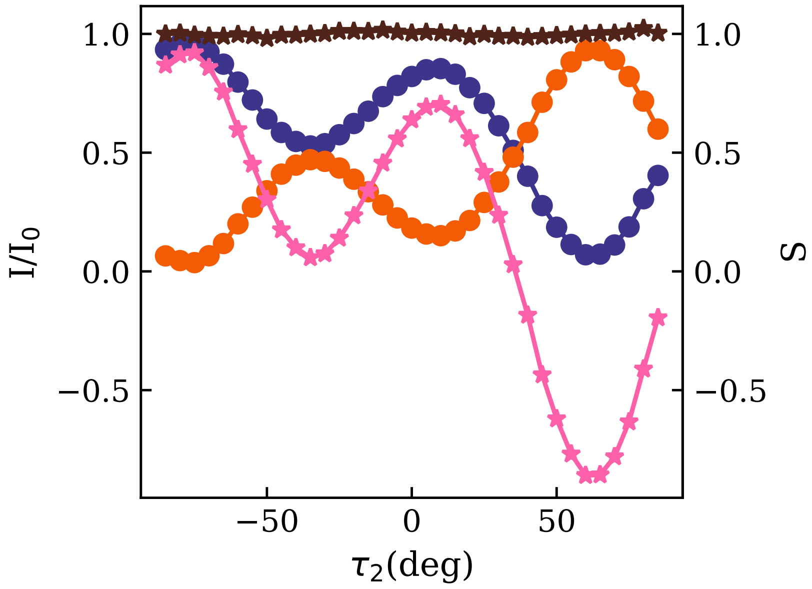


Figure 4.3: *Circles: Measured intensity (normalized) as function of second MPC paddle angle. The orange data was measured behind V1, the blue data behind H1. The other paddles were kept at constant angles $\tau_1 = -75°$, $\tau_3 = +5°$. Stars: calculated stokes parameters S_0 (brown) and S_1 (pink) as a function of second MPC paddle angle.*

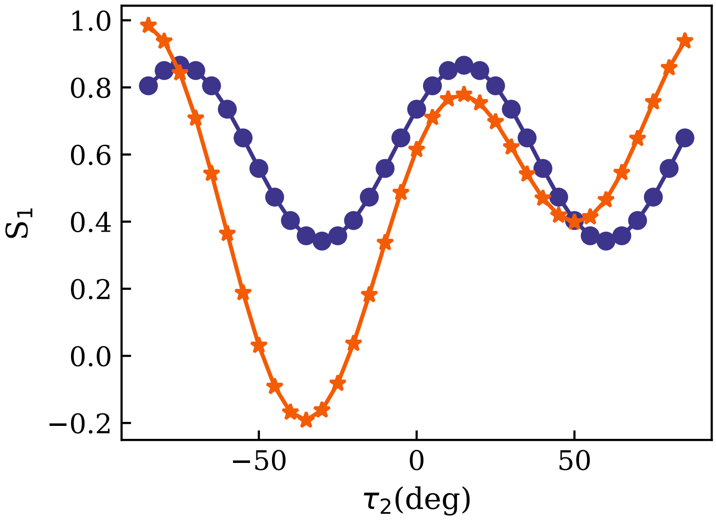


Figure 4.4: *Stokes parameter S_1 as a function of the MPC paddle angle w.r.t. the fast axis τ_2 modeled for a device with perfect retardance (i.e. $\delta_2 = \pi$, $\delta_4 = \pi/2$) (blue circles) and for one with imperfect retardance ($\delta_2 = 0.87\pi$, $\delta_4 = 2.62\pi$) (orange stars). The input was diagonally polarized in both cases and the other two paddle angles were kept constant at $\tau_1 = -75°$ and $\tau_3 = +5°$. For perfect retardance the maxima are at the same height and are 90° apart and the same between two minima. For imperfect retardance the maxima/minima are not of equal height and their spacing is also not exactly 90°.*

It is expected for a $\lambda/2$ waveplate that when the plate is rotated by 90° the polarization is equal. This would mean that the value of S_1 should be the same after a 90° rotation. However, this is clearly not the case since none of the (local) maxima or minima of S_1 are at the same value. Also the spacing between two local maxima is 95° and the spacing between two minima is 85°. The cause for this behaviour is that the paddles that we use are not perfect waveplates. Their retardance (see equation 4.2) differs from the perfect π and $\pi/2$ expected for $\lambda/2$ and $\lambda/4$ plates respectively.

In order to emphasize the impact imperfect retardance has on the effect the MPC has on changing the polarization state, we have modeled the MPC Mueller matrix acting on the stokes vector of diagonally polarized light. The result of this simulation is displayed in figure 4.4 where the value of Stokes parameter S_1 is plotted as function of MPC paddle angle τ_2. The blue circles represent the effect of an MPC where the retardance is the perfect $\delta_2 = \pi$ and $\delta_4 = \pi/2$. The orange stars represent the effect of an MPC paddle where the retardance matches the values from equation

4.2 which are the expected values for the MPC in the experiment. From this figure we can conclude that the behaviour of Stokes parameter S_1 in the measurement is a direct result of the imperfect retardance.

The goal of this more in depth assessment of the Motorized fiber Polarization Controllers was to get a better understanding of what happens inside the device, but also to see if we would be able to predict for which angles (τ_1, τ_2, τ_3) would result in one of the six interesting polarization states ($|H\rangle$, $|V\rangle$, $|D\rangle$, $|A\rangle$, $|R\rangle$, $|L\rangle$). The parameters which remain unknown are the Stokes parameters (S_1, S_2, S_3) of the input polarization state. The parameter S_0 is always set to 1, since it represents the total intensity. Even though a polarizer is used in the setup, the polarization changes into an unknown state due to the travel through the optical fibers.

By fitting the MPC Mueller matrix to the measured data we try to extract the unknown input polarization state. The result for one set of data is shown in figure 4.5 where the output Stokes parameter S_1 is plotted as function of angle τ_2. The pink stars is the measured data from figure 4.3. From this measured data the input Stokes parameters were extracted

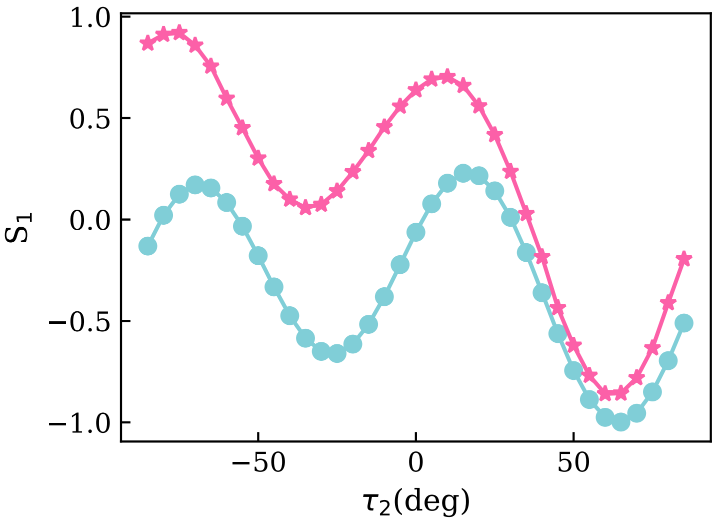


Figure 4.5: *Stokes parameter S_1 as a function of MPC second paddle angle τ_2. The measured data (pink stars) was fitted with the use of the Mueller matrix M_{MPC} to extract the input Stokes parameters S_1', S_2' and S_3'. These parameters were put back into the Mueller matrix to calculate the output Stokes parameter S_1 as function of MPC angle τ_2 (blue circles). The other MPC angles were set to fixed values $\tau_1 = -75°$ and $\tau_3 = +5°$. And the input Stokes parameters used for the model were $S_1' = 0.69$, $S_2' = 0.72$ and $S_3' = -0.07$.*

$S'_1 = 0.62 \pm 0.05$, $S'_2 = 0.64 \pm 0.06$ and $S'_3 = -0.02 \pm 0.05$. From the fit we have chosen a set of Stokes parameters which would form a pure state (i.e. $S_1^2 + S_2^2 + S_3^2 = 1$). With this set, $S'_1 = 0.69$, $S'_2 = 0.72$ and $S'_3 = -0.07$, the output Stokes parameter S_1 was calculated as a function of MPC angle τ_2 (blue circles).

The shape of the fit is quite similar to the measured data, but still is far off. There are several possible reasons why the fit does not follow the data closely. First of all, the total intensity fluctuates over the measurement as can be seen in figure 4.3. Moreover, the retardance δ_2 and δ_4 were calculated from given parameters, but have not been experimentally extracted. Therefore, there is the possibility that the used values in the fit are slightly off. Consequently, the fit would not follow the data either.

In the fit we have also assumed that the fast axis of the fiber (or the light through the fiber) is aligned with the 0° point defined for the MPC. If this assumption is incorrect, then the outcome of the fit will also change.

In conclusion, using the Mueller matrices for linear retarders has assisted in creating an understanding of what happens inside the MPC device. However, due to the unknown input Stokes parameters it is difficult to predict for which combination of τ_1, τ_2 and τ_3 leads to a certain polarization state. These devices have to be calibrated experimentally.

4.3 Calibration

In the previous section we have shown that bending and twisting an optical fiber alters the state of polarization. While this phenomenon is utilized in the MPCs it is also present in the fibers outside of the MPC. As a result the polarization state (which is known just after the polarizer) is scrambled into an unknown state throughout the setup. We described these unknown changes to the state of polarization with the use of unitaries. These unitaries are shown in figure 4.6.1 where U_1 to U_7 correspond to changes due to any unwanted stress-induced birefringence in the single-mode fibers. The unitaries U_{BS1} and U_{BS2} contain the operations performed by a 50:50 beamsplitter and the unitaries U_{MPC1}, U_{MPC2} and U_{FPC} are the operations performed by the fiber polarization controllers.

The setup needs to be calibrated to know the settings for which paddle angles of the Motorized fiber Polarization Controllers (the verifiers in the protocol) send out certain polarization states. In this thesis the setup has only been calibrated for the horizontal and vertical polarization states and only for a coherent light source.

The first step in this calibration process in shown in figure 4.6.2. This is

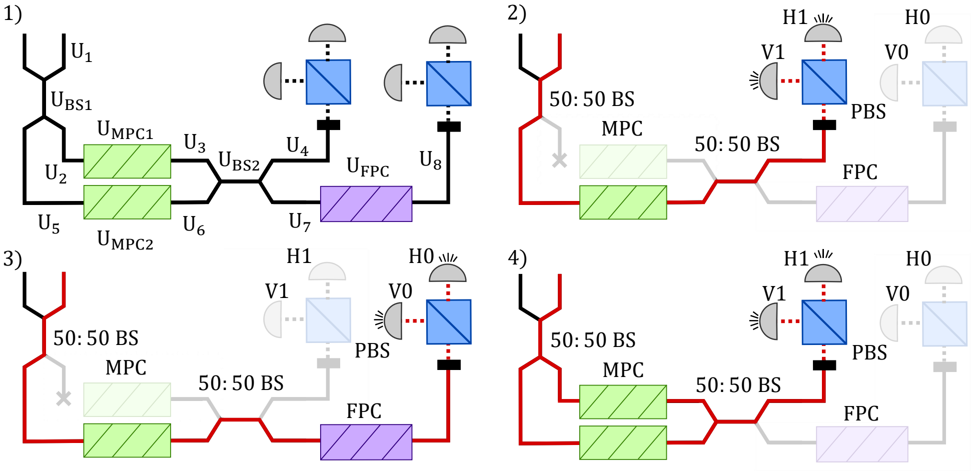


Figure 4.6: *Schematic representation of the setup without the laser and polarizer part displaying: 1) All the unitaries acting on the polarization state of the light travelling through the system. 2) The first step in the calibration where one MPC is characterized by measuring the intensities at outputs H1 and V1 while rotating the three angles. 3) The second step of the calibration where the FPC is calibrated. The MPC is set to a single polarization (either H or V) and the intensities are measured at outputs H0 and V0. The FPC paddles are rotated until H0 and V0 give the same output as was measured at H1 and V1. 4) The final step in the calibration process where the second MPC is reattached and its paddles are rotated until maximum visibility has been detected. The visibility is measured by measuring the intensities behind the outputs H1 and V1.*

the MPC measurement described in the previous section where the intensities of the light through a single MPC are measured at outputs H1 and V1. The red line depicts the path taken by the light from the source to the outputs (the light travels from left to right). As explained before, the intensity of the H and V polarization components of the light are measured as a function of the three paddle angles τ_1, τ_2 and τ_3. From this measurement the set of angles is found where the light is either H or V polarized.

For example, if the light travelling through MPC2 for a certain set of paddle angles τ leads to a maximum intensity measured at V1 and minimum intensity at H1 it would mean that:

$$U_4\, U_{BS2}\, U_6\, U_{MPC2}\, U_5\, U_{BS1}\, U_1\ |\Psi\rangle = |V\rangle \tag{4.5}$$

From this it is clear that only the state which arrives at the PBS is known. Consequently, the state which in this thesis we will call vertically polarized means that the light was vertically polarized when arriving at the polarizing beamsplitter. This does not mean that the state of polarization of the same light has to be vertically polarized when arriving at the second fibersplitter.

For the prover to be able to perform the Bell-State measurement and to return the correct result the state arriving at the two PBS must be the same. In other words, if the light is fully reflected by the PBS into detector V1, then the light should also be fully reflected by the other PBS into detector V0. As a result the unitaries transformations in both paths between the second fibersplitter and the two polarizing beamsplitters must be equal (eq 4.6).

$$U_8 \, U_{FPC} \, U_7 \, |\Psi\rangle = U_4 \, |\Psi\rangle \tag{4.6}$$

This condition is achieved in the second step of the calibration process (fig 4.6.3). First the angles for the MPC are set that the output behind H1 and V1 displays the result for either H or V polarized light. Then the intensities are measured behind the other PBS at outputs H0 and V0. By manually rotating the three paddles of the FPC the same outcome is generated for the other PBS.

The third and final step in the calibration process is to add the other MPC to the system (see fig 4.6.3). The intensities are again measured at outputs H1 and V1. The MPC which was already attached (MPC2) has its paddles set such that the light is vertically polarized. Then the paddles of the newly attached MPC (MPC1) are rotated while the paddles of MPC remained fixed.

The setup in combination with using a coherent light source results in a Mach-Zehnder type of interference. The visibility of the interference is maximum when the coherent light arriving at the second fibersplitter is indistinguishable. Hence, changing the polarization by rotating the paddles of MPC1 while keeping MPC2 constant changes the visibility of the interference. By monitoring the visibility while changing the paddles of MPC1 we found the maximum value which suggests that the polarization from both MPC1 and MPC2 is equal. Then the same steps are done for the horizontal polarization.

4.4 Results

In this section we characterise the loss in the setup and calibrate it for horizontal and vertical polarization states. To characterise the loss through the setup, the power has been measured at different points through the setup.

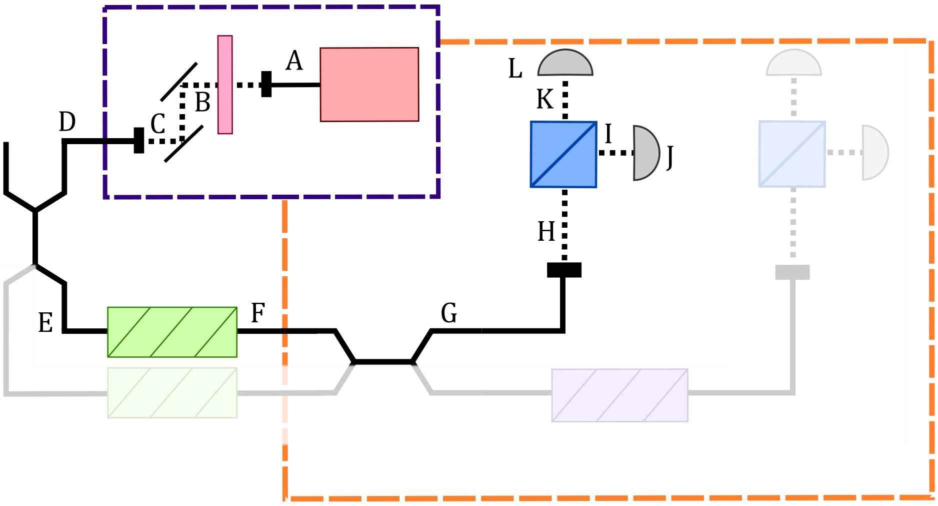


Figure 4.7: *Schematic representation of the setup (for labels see figure 4.1), with the positions where the power was measured are annotated by the letters A-L.*

These positions are highlighted in figure 4.7 and the result is displayed in table 4.1. We measured the power using a Thorlabs PM100D and only one MPC (MPC1) was attached to the setup during these measurements. The table also displays the percentage of the measured power is with respect to the source (position A), after coupling the light from free-space to single-mode fiber (position D) and in front of the PBS (postion H).

The polarizer was rotated while monitoring the power at position B and was set in the position where the measured power was at its maximum (11.4mW). This maximum is only 78.6% of the power measured in position A, implying that the light source is not fully polarized in one single direction. Most of the power was lost in coupling the light from free-space into a single-mode fiber. Fortunately, the free-space part behind the source is only needed for coherent light. The single photon sources (SPDC or quantum dots) create photons in a single pure polarization state. Therefore, this part of the setup can be discarded when transitioning to such a light source.

The intensity of the light before and after a fibersplitter (between positions D and E and F and G) is (more than) halved. This halving of the power is due to the fibersplitters splitting the light into two paths 50:50. This is only the case when one of the two MPCs is not attached to the system. When both MPCs are attached, the power is only halved for the first fibersplitter, but at the second fibersplitter there would be two inputs with equal intensity. In this case the intensity in point G would be similar to the intensity at position F.

Behind the Polarizing Beamsplitter the light is split into its horizontal and vertical component. Therefore, in principle the power measured at positions I and K should together be the value measured at position H. However, this is clearly not the case. The cause of this discrepancy is due to the efficiency of the PBS. The reflection efficiency of the PBS is approximately 99.5%, while its transmission efficiency is approximately 90%. When taking this into account the power measured at position K should be around 70% of the power at H instead of 63.4%. Then the sum of the power measured behind the PBS would be equal to the power before the PBS.

For the first step of the calibration process only one MPC is attached to the setup. By performing the MPC measurement we have found the paddle angles for which the light is either vertically or horizontally polarized when arriving at the PBS. These angles τ for MPC2 are displayed in table 4.2 together with the intensity measured by the photodiodes. The measured intensities are compensated for the background values of the photodiodes (-0.0106 for H1 and -0.0054 for V1).

Position	Power	% w.r.t. source	% w.r.t. D	% w.r.t. H
A	14.5mW	100%		
B	11.4mW	78.6%		
C	9.46mW	65.2%		
D	1.79mW	12.3%	100%	
E	691μW	4.8%	38.6%	
F	447μW	3.1%	25.0%	
G	221μW	1.5%	11.8%	
H	205μW	1.4%	11.5%	100%
I	62.5μW	0.43%	3.49%	30.5%
J	55.0μW	0.37%	3.07%	26.8%
K	130μW	0.90%	7.26%	63.4%
L	127μW	0.88%	7.09%	62.0%

Table 4.1: *Table of the power measured at different positions in the setup. These positions are shown in figure 4.7. The measured power at each position is also expressed as percentage w.r.t. the source, position D when the light is coupled back into the single mode fiber after the polarizer and position H where the light is coupled out of the single mode fiber before travelling into the PBS.*

Pol	τ_1	τ_2	τ_3	I_{H1}	I_{V1}
V	$-26°$	$+85°$	$-85°$	0.000	0.115
H	$+33°$	$-39°$	$-82°$	0.096	0.001

Table 4.2: *Table of angles τ of MPC2 with the intensities measured at outputs H1 and V1 where the measured polarization is either vertical or horizontal. The intensities were measured with the use of the Thorlabs photodiodes PDA10A-EC.*

The second step in the calibration process was rotating the manual Fiber Polarization Controller (FPC) such that the transformation on the polarization state in the path to H1 and V1 is equal to the transformation in the path to H0 and V0. The angles for this are more difficult to obtain quantitatively and are therefore not mentioned in the thesis. The MPC2 was set such that vertical polarized light was detected, i.e. the intensity measured at H1 was 0. The proposed method to calibrate the FPC is to first rotate the second paddle until a minimum value is obtained at H0. Then the two outer paddles are moved sequentially until a further minimum is found. It is a method that needs several iterations most of the time.

The final step in the calibration process is to reattach MPC1 and to find out where for this polarization controller the polarization is either equal or opposite to the polarization state created by MPC2. It is important to have performed the previous two steps completely before moving to the final step. Disconnecting and reconnecting the single mode fibers results in changes in the transformation unitary U_2 (see figure 4.6.1) and the system needs to be recalibrated. The MPC2 was set to create vertical polarized photons. The intensity of the light is again measured behind outputs H1 and V1 with the use of the photodiodes.

When connecting the MPC1 to the rest of the setup, two changes appear in the intensity measured. First of all, the intensity measured increases and secondly the intensity fluctuates. The increase in intensity is caused by the fact that now the second fibersplitter has both inputs

	MPC1			MPC2		
Pol	τ_1	τ_2	τ_3	τ_1	τ_2	τ_3
V	$+1°$	$-1°$	$+0°$	$-26°$	$+85°$	$-85°$
H	$-47°$	$-2°$	$+42°$	$+33°$	$-39°$	$-82°$

Table 4.3: *Table of angles τ for both Motorized Fiber Polarization Controllers where the output polarization is measured to be either horizontal or vertical.*

and both outputs in operation instead of only one input and two outputs. Hence, the intensity of the light is not only split into two paths as in the first step of the calibration. Instead the light of the two paths are interfering. This leads to the cause of the fluctuations in intensity. When there is overlap in the state of light, the two paths interfere inside the 50:50 fibersplitter. The interference fringes are caused by the phase difference between the two paths. In our case it is the thermal fluctuations which cause the phase difference, this enables us to evaluate the interference contrast.

By luck, the unitaries operating on the light travelling between the source and MPC1 changed the polarization state very close to vertical polarization. Therefore, the changes on the paddles are very small for the vertical state as shown in table 4.3. In this table the angles τ for both MPC1 and MPC2 are displayed for the vertical and horizontal polarization state.

The combination of angles τ of MPC1 for the horizontal polarization state were found by rotating the paddles while keeping the angles of MPC2 fixed for vertical polarization. In this case, there should be no overlap in the polarization state of the light from both polarization controllers. As a result, there should be no interference fringes. The fluctuation of the intensity was monitored while rotating the paddles of MPC1. This result was then verified by rotating MPC2 into its horizontal state configuration and the interference fringes returned as expected.

The measured interference fringes are displayed in figure 4.8. The intensity at output H1 (blue) and V1 (orange) were measured in 10 second time increments. The fringes were monitored for four different MPC configuration combinations: (VV case) both MPCs set for the vertical state (4.8.a), (VH case) MPC1 set for the vertical state and MPC2 for the horizontal state (4.8.b), (HV case) MPC1 set for the horizontal state and MPC2 for the vertical state (4.8.c) and (HH case) both MPCs set for the horizontal state (4.8.d). The plotted intensities have been compensated for the asymmetric efficiency of the PBS and the background of the photodiodes.

From the measured data we obtained the visibility of the interference fringes by dividing the difference between the maximum and minimum intensity by the sum of them (eq 2.12). When the polarization state at both inputs of the fibersplitter are equal (figures 4.8.a and 4.8.d) the interference fringes are large for the one polarization while the intensity on the other is almost 0. For the vertical polarization the average value measured at H1 is 0.002, while the output V1 oscillated between 0.032 and 0.465 giving a visibility of $\mathcal{V}_{VV} \approx 0.87$. For the horizontal polarization the average value measured at V1 is 0.003, while the intensity at H1 oscillated between 0.026 and 0.451 resulting in a visibility of $\mathcal{V}_{HH} \approx 0.85$.

In both the VV and HH cases the visibility is not 1, meaning that the light arriving at the two inputs of the fibersplitter is not completely indistinguishable. However, the lack of overlap can not be explained when only looking at the polarization states. In both cases the intensity of the opposite polarization state is close to zero and barely fluctuates over time. This suggests that the lack of overlap is caused in another mode of the photon state. The timing of the light at the inputs for example, since the

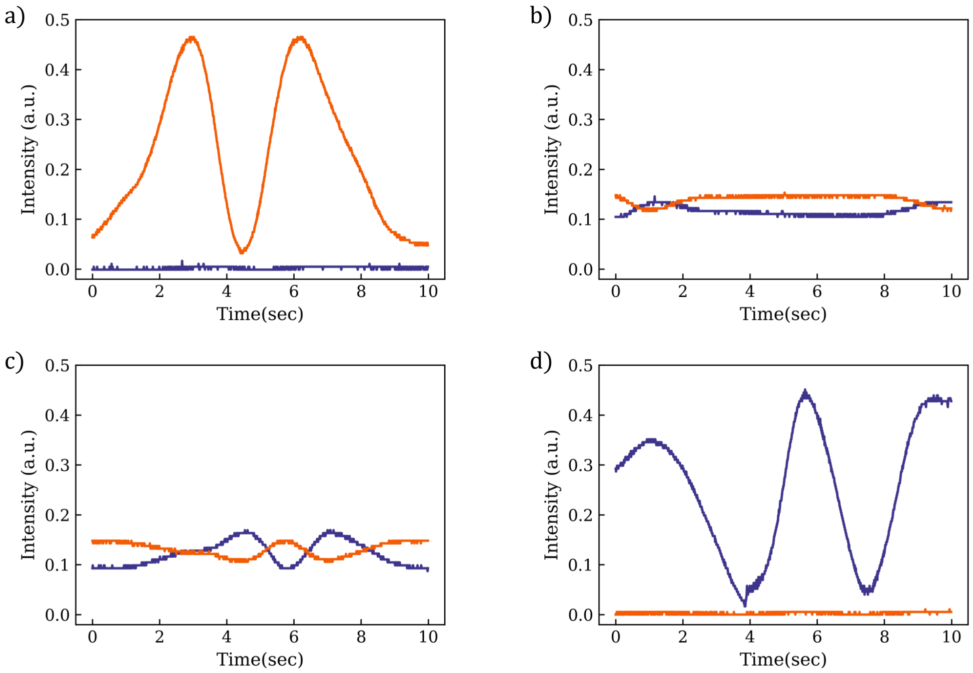


Figure 4.8: *Intensity measured at outputs H1 (orange) and V1 (blue) as a function of time. Both MPCs are connected and the oscillations as function of time are a result of phase changes due to thermal fluctuations. a) MPC1 and MPC2 set to vertical polarization (VV case). The intensity at output V1 fluctuates between* 0.032 *and* 0.465 *resulting in a visibility of* $\mathcal{V}_{VV} \approx 0.87$*, while the average intensity at H1 is* 0.002*. b) MPC1 set to vertical and MPC2 to horizontal polarization (VH case). The intensity at V1/H1 oscillates between* 0.116 *and* 0.153*, and* 0.105 *and* 0.146 *respectively, resulting in visibilities* $\mathcal{V}_{VH,V} \approx 0.14$ *and* $\mathcal{V}_{VH,H} \approx 0.16$*. c) MPC1 set to horizontal and MPC2 to vertical polarization (HV case). The intensity at V1/H1 oscillates between* 0.106 *and* 0.148*, and* 0.087 *and* 0.169 *respectively, resulting in visibilities* $\mathcal{V}_{HV,V} \approx 0.17$ *and* $\mathcal{V}_{HV,H} \approx 0.32$*. d) MPC1 and MPC2 set to horizontal polarization (HH case). The intensity at output H1 fluctuates between* 0.021 *and* 0.451*, resulting in a visibility of* $\mathcal{V}_{HH} \approx 0.85$*, while the intensity at V1 is* 0.003*.*

single-mode fibers are never of the exact same length the timing of the photons arriving at the fibersplitter can be off. This also leads to a phase difference and reduces the visibility.

When the polarization at both inputs of the second fibersplitter are orthogonal (the VH and HV cases), there should be no overlap in the photonstates and, as a result, the visibility should be close to zero. For the VH case (figure 4.8.b), where MPC1 is set to the vertical polarization configuration and MP2 to horizontal polarization, the light at output V1 fluctuated between 0.116 and 0.153, resulting in a visibility of $\mathcal{V}_{VH,V} \approx 0.14$. The light at output H1 fluctuated between 0.105 and 0.146, resulting in a visibility of $\mathcal{V}_{VH,H} \approx 0.16$. These visibilities are very close to each other, but are not quite zero. This is most probably caused by another mode space of the photon state as discussed for the HH and VV cases.

Contrary to the VH case, the visibilities for the HV (figure 4.8.c) case differ much more from each other. At V1 the intensity fluctuates between 0.106 and 0.148 giving a visibility of $\mathcal{V}_{HV,V} \approx 0.17$ which is still close to the visibilities $\mathcal{V}_{VH,V}$ and $\mathcal{V}_{VH,H}$. However, the visibility at H1, where the intensity fluctuated between 0.087 and 0.169, is twice the value of $\mathcal{V}_{HV,H} \approx 0.32$. This difference is unexpected and we cannot account for the cause as of yet.

In conclusion, we are able to build a setup intended for QPV and calibrate it for horizontal and vertical polarized light. The overlap between the photon states is large for equal polarization and relatively small for the opposite polarization.

Chapter 5

Conclusion and Discussion

In this thesis we described the first steps for a demonstration experiment for a Quantum Position Verification (QPV) scheme. QPV uses a combination of quantum mechanics (no cloning theorem) and special relativity (information cannot travel faster than the speed of light). We assumed a one-dimensional system where there are two verifiers V_0 and V_1 and one prover P who is exactly in the middle. The discussed protocol has been proposed by Lim et al. [7] and it utilizes the polarization state of single photons as the carrier of quantum information. This particular protocol requires the prover perform a probabilistic projection onto a Bell-State.

We expanded the existing protocol to account for the effects caused by photon loss in the quantum channels and errors in the polarization state and simulated the success rate as a function of both. From these simulations we can conclude that high photon loss can lead to problematic scenarios such as the verifiers not being able to distinguish the error produced by an honest or dishonest prover. The simulations also show that when the verifiers set the quota threshold (n_{th}) at a fixed level, the verifiers need to have accurate knowledge on and control of the transmission of the used channels.

In our first steps towards experimental QPV, we have build a fiber based setup using a coherent light source (see figure 4.1). The Motorized fiber based Polarization Controllers (MPC), which represent the verifiers in the setup, have been investigated. We measured the intensity for horizontal and vertical polarization from which we calculated the Stokes parameter S_1. The measured data was then compared to the theory of stress-induced birefringence in single-mode optical fibers.

Due to the fact that stress-induced birefringence happens everywhere inside single-mode fibers there was the problem that after the initial free-space polarizer the polarization state of the light was unknown. Hence, we designed a three step calibration process to calibrate the actions of the verifiers (the MPCs). By performing the calibration for horizontal and vertical polarization states, we have shown that with the current setup we are able to produce an overlap of approximately 85% between the equal polarization states at the input of the Bell-State projection. This overlap is sufficiently accurate to distinguish an honest prover from the LOCC attackers, because a visibility of 0.85 leads to an error rate of 0.15 remaining below the minimum error of the attackers of 1/4.

The first next step towards experimental Quantum Position Verification will be to calibrate the existing setup for other polarization state (diagonal and anti-diagonal linear polarized light, right-handed and left-handed circular polarized light).

At some point, the coherent light source needs to be switched to a single photon source. Here the decisions on which single photon source and if it is only a single photon source or a combination of a single photon source and a weak coherent light source need to be made. When we switch to single photons, the verifiers will need to be able two switch between polarization states fast, since the source can create single photons in the MHz regime. The MPCs are definitely not fast enough and therefore faster ways to modify the polarization states for single photons need to be used, such as electro-optic modulators.

While working on the experimental side of QPV we are also searching for a protocol where Quantum Position Verification is used in combination with Quantum Key Distribution (QKD). In this case the QPV would be used to authenticate a communication channel between the verifiers and the prover and share a key at the same time.

Appendix A

Density Matrix Formalism

For the two input states we have the following pure polarization states:

$$\begin{aligned} |\Psi\rangle &= a\,|H\rangle + b\,|V\rangle \\ |\Phi\rangle &= u\,|H\rangle + v\,|V\rangle \end{aligned} \tag{A.1}$$

where $a, b, u, v\ \epsilon\ \mathbb{C}$. A 50:50 beamsplitter has two input paths (0,1) and has two output paths (2,3). The photon from path 0 is described by the state $|\Psi\rangle$ and the photon from path 1 is described by $|\Phi\rangle$. We take these two photons to be distinguishable for the time being. Hence, the joined input state can be described as:

$$|in\rangle = au\,|H_0H_1\rangle + av\,|H_0V_1\rangle + bu\,|V_0H_1\rangle + bv\,|V_0V_1\rangle \tag{A.2}$$

here the subscript shows the path the photon takes and the first term in the ket is the photon belonging to $|\Psi\rangle$ and the second term belongs to $|\Phi\rangle$.

The transformation of the state due to the 50:50 beamsplitter is defined in the following way:

$$\begin{aligned} \hat{a}_0^\dagger &= \frac{1}{\sqrt{2}}(\hat{a}_2^\dagger + i\hat{a}_3^\dagger) \\ \hat{a}_1^\dagger &= \frac{1}{\sqrt{2}}(i\hat{a}_2^\dagger + \hat{a}_3^\dagger) \end{aligned} \tag{A.3}$$

where $\hat{a}^\dagger$ is the creation operator. In order to take the polarization into account in this formalism we define the creation operator of a horizontal polarized photon is such a way that: $|H_0\rangle = \hat{a}_{0,H}^\dagger$.

Using the input state and the transformation equations results in the following output state:

$$\begin{aligned}
&|out\rangle = \\
&\frac{1}{2}\, au\ (i\,|H_2H_2\rangle + |H_2H_3\rangle - |H_3H_2\rangle + i\,|H_3H_3\rangle) \\
&+\frac{1}{2}\, av\ (i\,|H_2V_2\rangle + |H_2V_3\rangle - |H_3V_2\rangle + i\,|H_3V_3\rangle) \\
&+\frac{1}{2}\, bu\ (i\,|V_2H_2\rangle + |V_2H_3\rangle - |V_3H_2\rangle + i\,|V_3H_3\rangle) \\
&+\frac{1}{2}\, bv\ (i\,|V_2V_2\rangle + |V_2V_3\rangle - |V_3V_2\rangle + i\,|V_3V_3\rangle)
\end{aligned} \tag{A.4}$$

$$\begin{aligned}
&|out\rangle = \frac{1}{2}(\\
&i[au\,|H_2H_2\rangle + au\,|H_3H_3\rangle + bv\,|V_2V_2\rangle + bv\,|V_3V_3\rangle] \\
&+i(av+bu)[|H_2V_2\rangle + |H_3V_3\rangle] \\
&+(av-bu)[|H_2V_3\rangle - |V_2H_3\rangle])
\end{aligned} \tag{A.5}$$

Since this output state consists of 16 terms, the corresponding density matrix is of size 16x16. Due to this size the full density matrix is not shown.

The (diagonal) elements of the density matrix are the probabilities to have one of the three possible answers dictated by the protocol (z=0,1,ø).

$$\begin{aligned}
z = 0 &: \rho_{H_2V_2} + \rho_{V_2H_2} + \rho_{H_3V_3} + \rho_{V_3H_3} \\
z = 1 &: \rho_{H_2V_3} + \rho_{V_3H_2} + \rho_{H_3V_2} + \rho_{V_2H_3} \\
z = ø &: \rho_{H_2H_2} + \rho_{H_2H_3} + \rho_{H_3H_2} + \rho_{H_3H_3} \\
&\quad +\rho_{V_2V_2} + \rho_{V_2V_3} + \rho_{V_3V_2} + \rho_{V_3V_3}
\end{aligned} \tag{A.6}$$

Remember that this formalism was for two photons which were distinguishable. However, in the experiment the photons are indistinguishable giving rise to the possibility of quantum interference. As a result, not all off-diagonal elements of the density matrix can be discarded. The cross-terms like $|H_2V_2\rangle\langle V_2H_2|$ also need to be added to the outcome probabilities. Moreover, the values for the diagonal terms of $|H_2H_2\rangle$, $|V_2V_2\rangle$, $|H_3H_3\rangle$, $|V_3V_3\rangle$ in the density matrix need to be multiplied by a factor two due to the fact that $\hat{a}^\dagger_{2,H}\hat{a}^\dagger_{2,H}|0,0\rangle = \sqrt{2}\,|2H,0\rangle = \sqrt{2}\,|H_2H_2\rangle$ for indistinguishable photons.

Taking this into account, the probabilities for the three answers of the bell-state measurement are:

$$
\begin{aligned}
z = 0 &: \frac{1}{2}(|a|^2|v|^2 + ab^*u^*v + a^*buv^* + |b|^2|u|^2) \\
z = 1 &: \frac{1}{2}(|a|^2|v|^2 - ab^*u^*v - a^*buv^* + |b|^2|u|^2) \\
z = ø &: \frac{1}{2}(2|a|^2|u|^2 + 2|b|^2|v|^2)
\end{aligned}
\tag{A.7}
$$

Appendix B

Error coefficient

This chapter is a more detailed derivation of the relation between the polarization states and the defined error coefficient R.

An error in the measurement by the honest prover is possible when the polarization states are not perfectly orthogonal. In order to simulate this, two tunable phases (γ and ϵ) are added to the expression of $|\Phi\rangle$. The expression for $|\Psi\rangle$ remains unchanged.

$$|\Phi\rangle = \cos\left(\frac{\theta+\gamma}{2}\right)|H\rangle + (\cos(\omega+\epsilon) + i\ \sin(\omega+\epsilon))\sin\left(\frac{\theta+\gamma}{2}\right)|V\rangle$$

In this derivation we assumed that both verifiers want to sent out a diagonal polarized photon. This means that the conclusive result send back by the honest prover is z=0 with probability $\frac{1}{2}$. Therefore, only P_0 is used in this derivation. Inserting $|\Psi\rangle$ and $|\Phi\rangle$ into P_0 gives the following:

$$\begin{aligned}
P_0 = \frac{1}{2}\Bigg[&\cos^2\left(\frac{\theta}{2}\right)\sin^2\left(\frac{\theta+\gamma}{2}\right) \\
&+\cos\left(\frac{\theta}{2}\right)(\cos\phi - i\ \sin\phi)\sin\left(\frac{\theta}{2}\right)\cos\left(\frac{\theta+\gamma}{2}\right)(\cos(\omega+\epsilon)+i\ \sin(\omega+\epsilon))\sin\left(\frac{\theta+\gamma}{2}\right) \\
&+\cos\left(\frac{\theta}{2}\right)(\cos\phi + i\ \sin\phi)\sin\left(\frac{\theta}{2}\right)\cos\left(\frac{\theta+\gamma}{2}\right)(\cos(\omega+\epsilon)-i\ \sin(\omega+\epsilon))\sin\left(\frac{\theta+\gamma}{2}\right) \\
&+\sin^2\left(\frac{\theta}{2}\right)\cos^2\left(\frac{\theta+\gamma}{2}\right)\Bigg]
\end{aligned}$$

Since both verifiers send out D-polarized photons we can state that $\theta = \frac{\pi}{2}$, $\phi = 0$ and $\omega = 0$ leading to:

$$P_0 = \frac{1}{2}\left[\frac{1}{2}\sin^2\left(\frac{\frac{\pi}{2}+\gamma}{2}\right) + \frac{1}{2}\cos\left(\frac{\frac{\pi}{2}+\gamma}{2}\right)\sin\left(\frac{\frac{\pi}{2}+\gamma}{2}\right)[\cos(\epsilon)+i\ \sin(\epsilon)]\right.$$
$$\left. + \frac{1}{2}\cos\left(\frac{\frac{\pi}{2}+\gamma}{2}\right)\sin\left(\frac{\frac{\pi}{2}+\gamma}{2}\right)[\cos(\epsilon)-i\ \sin(\epsilon)] + \frac{1}{2}\cos^2\left(\frac{\frac{\pi}{2}+\gamma}{2}\right)\right]$$

$$\begin{aligned} P_0 &= \frac{1}{4}\left[1+2\ \cos\left(\frac{\frac{\pi}{2}+\gamma}{2}\right)\sin\left(\frac{\frac{\pi}{2}+\gamma}{2}\right)\cos(\epsilon)\right] \\ &= \frac{1}{4}\left[1+\cos(\gamma)\cos(\epsilon)\right] \end{aligned}$$

We defined R in such a way that $R = 0$ (no error) means that the probability of measuring the correct answer is $\frac{1}{2}$. When there is maximum error $R = 1$, the probability of measuring the correct answer should be 0. Therefore, the relation between P and R can be defined as:

$$P_{i=0,1} = \frac{1}{2}(1-R)$$

And as a result the relation between the angles γ and ϵ and the error coefficient R is:

$$\cos(\gamma)\cos(\epsilon) = 1-2R$$

Please note that this expression is symmetric for γ and ϵ. Hence, for simplicity's sake, $\epsilon = 0$ in the simulations. Also note that, even though the derivation is for P_0, the expression is exactly the same for P_1, since in that case $\omega = \pi$.

Acknowledgements

First and foremost, I wish to express my sincere appreciation to my supervisor, Wolfgang Löffler, who has given me the opportunity to build an experimental project from the ground up. Without his endless knowledge in may aspects of (quantum) optics and his ability to perform black magic in the lab I would not have come as far as I have. I also would like to thank Professor Harry Buhrman for his conversations with Wolfgang resulting in the collaboration between the two research groups, and to thank him for his boundless enthusiasm shown throughout the year.

Furthermore, I wish to show my gratitude towards Florian Speelman, René Allerstorfer and Philip Verduyn Lunel, the students from the Buhrman group, for aiding me in understanding the theory side of QPV and for asking all the right questions. The PhD students in my own group, Petr Steindl and Matteo Fisicaro, I want to thank for the help they have provided in the lab, especially during the alignment process of the setup. From the Electronics Department I want to thank Arno van Amersfoort for his device which enables us to create the three different answers the prover in the protocol has to return to the verifiers.

I appreciate all the people of the Quantum Optics department for all the discussions we have had about my project, but also about research in general. I also want to thank them for all the fun times that made the frustrating moments much more bearable. And last, but not least, I want to thank my friends and family who remind me that it is allowed to take breaks and recharge before diving back into work.

I am looking forward to continue this research for my PhD and to keep on working together with everyone involved for the next couple of years.

Bibliography

[1] A. Kent, W. J. Munro, and T. P. Spiller, *Quantum tagging: Authenticating location via quantum information and relativistic signaling constraints*, Physical Review A - Atomic, Molecular, and Optical Physics **84**, 1 (2011).

[2] R. A. Malaney, *Quantum location verification in noisy channels*, GLOBECOM - IEEE Global Telecommunications Conference , 1 (2010).

[3] R. A. Malaney, *Location-dependent communications using quantum entanglement*, Physical Review A - Atomic, Molecular, and Optical Physics **81**, 1 (2010).

[4] N. Chandran, V. Goyal, R. Moriarty, and R. Ostrovsky, *Position Based Cryptography*, Cryptology ePrint Archive, Report 2009/364, 2009, `https://eprint.iacr.org/2009/364`.

[5] H. Buhrman, N. Chanan, S. Fehr, R. Gelles, V. Goyal, R. Ostrovsky, C. Schaffner, and P. Rogaway, *Position-based quantum cryptography: impossibility and constructions*, in *Lecture notes in computer science*, volume 6841 of *Lecture Notes in Computer Science*, pages 429–446, Springer, Berlin, Heidelberg, 2011.

[6] S. Beigi and R. König, *Simplified instantaneous non-local quantum computation with applications to position-based cryptography*, New Journal of Physics **13** (2011).

[7] C. C. W. Lim, F. Xu, G. Siopsis, E. Chitambar, P. G. Evans, and B. Qi, *Loss-tolerant quantum secure positioning with weak laser sources*, Physical Review A **94** (2016).

[8] J. A. J. A. Jones and D. Jaksch, *Quantum information, computation and communication*, Cambridge University Press, Cambridge, [UK] ; New York, 2012.

[9] H. Poincaré, *Leçons sur la théorie mathématique de la lumière. , Théorie mathématique de la lumière. II, Nouvelles études sur la diffraction, théorie de la dispersion de Helmholtz : leçons professées pendant le premier semestre 1891-1892 / par H. Poincaré,... ; rédigé*, Paris, Paris, 1892.

[10] E. Hecht, *Optics*, Always learning, Pearson, 4 edition, 2014.

[11] J. C. del Toro Iniesta, *Introduction to Spectropolarimetry*, Cambridge University Press, Cambridge, 2003.

[12] C. K. Hong, Z. Y. Ou, and L. Mandel, *Measurement of subpicosecond time intervals between two photons by interference*, Physical Review Letters **59**, 2044 (1987).

[13] C. Gerry and P. Knight, *Introductory Quantum Optics*, Cambridge University Press, 2004.

[14] E. Chitambar, D. Leung, L. Mančinska, M. Ozols, and A. Winter, *Everything You Always Wanted to Know About LOCC (ButWere Afraid to Ask)*, Communications in Mathematical Physics **328**, 303 (2014).

[15] R. Ulrich, S. C. Rashleigh, and W. Eickhoff, *Bending-induced birefringence in single-mode fibers*, Opt. Lett. **5**, 273 (1980).

[16] Thorlabs, *MPC220 and MPC320 Motorized Fiber Polarization Controller User Guide*, 2019, Available at: `https://www.thorlabs.com/thorproduct.cfm?partnumber=MPC320`.

[17] R. Ulrich and A. Simon, *Polarization optics of twisted single-mode fibers*, Appl. Opt. **18**, 2241 (1979).

[18] D. Tentori, A. Garcia-Weidner, and C. Ayala-Díaz, *Birefringence matrix for a twisted single-mode fiber: Photoelastic and geometrical contributions*, Optical Fiber Technology **18**, 14 (2012).