Discrete-Event Simulations of Quantum Random Walks, Quantum Key Distribution, and Related Experiments

von

Madita Franziska Nocon

Masterarbeit in Physik

vorgelegt der

Fakultät für Mathematik, Informatik und Naturwissenschaften
der RWTH Aachen

im September 2016

angefertigt im

Jülich Supercomputing Center
Forschungszentrum Jülich

bei

Prof. Dr. Kristel Michielsen

Prof. Dr. Stefan Wessel

Contents

1 Introduction

Nowadays computer simulations become increasingly important in science as they can be applied in cases where an experiment is (still) impossible or too expensive to be performed. Furthermore, if experiments are feasible, experimental outcomes and simulation results can be compared to help improving the experiment. In addition to that, when a theoretical calculation becomes too complicated to be solved analytically without too many assumptions, approximations, and simplifications, the solution can only be obtained numerically. However, for these kinds of simulations the theory which describes the field of study has to be well-known.

The connections between theory and experiment are clear: On the one hand, experiments provide data from which a theory can eventually be extracted that describes the outcomes of the experiments. On the other hand, from the theory predictions can be made which can be verified or disproved by experiments.

But how can we apply computer simulations if the theory is not yet completely understood or we do not want to rely on the theory for some reason? Basically, there are two possibilities. First, we can directly try to simulate the outcomes of performed experiments by applying "rules" which are not based on a theory, but lead to the same outcomes as the experiments (discrete-event simulation). The second possibility is to generate patterns by simple programs and look for corresponding results in experiments or resembling patterns in nature (cellular automata such as Lattice-gas cellular automata [1], Conway's *Game of life*[2], and the like). The links between theory, experiment, and simulation are visualized and summarized in Fig. 1.1.

In this thesis, we focus on the first of the two methods, the discrete-event simulation. Although in our case the theory (quantum theory) is well-known and successful, if not necessarily completely understood (e.g. see the quantum measurement paradox [3]), we apply the discrete-event simulation method to show that at least some results and effects of quantum theory such as single-particle interference can also be reproduced without the need of wave functions and the time-dependent Schrödinger equation. The discrete-event

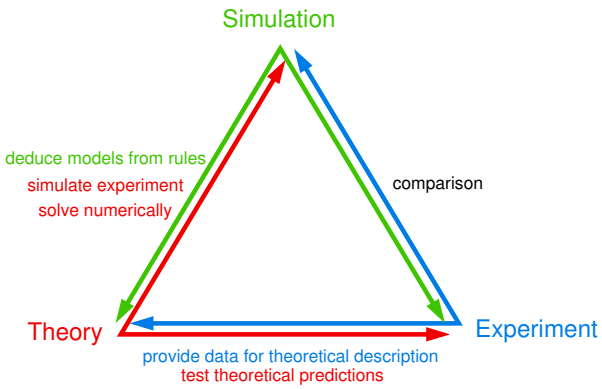

Figure 1.1: Visualization of the connections between theory, experiment, and simulation.

simulation method comes with a particle-only model without the need of particle-wave duality.

The simulation method applies to the period between a particle's creation and its detection. Quantum theory cannot describe what happens to the particle between its creation and detection. For example, in the case of a Mach-Zehnder interferometer experiment, quantum theory cannot predict with certainty at which detector a particle will be detected or how it actually travels through the interferometer. Quantum theory can only probabilistically predict the result at the measurement device, but it cannot describe how the results come about or interference patterns build themselves up detection event by detection event. For this reason, quantum theory and the discrete-event simulation method do not contradict each other.

Although the Copenhagen interpretation has become the most widely accepted interpretation of quantum theory, it does not have to be the only working interpretation to explain how observations such as single-particle interference can be understood. There are indeed other interpretations of quantum theory, such as Einstein's statistical interpretation [4], the Bohmian interpretation [5] [6], the many-worlds interpretation [7], the spontaneous collapse interpretation [8], and others. To some extent, one has to believe in one or the other interpretation as there is not yet any satisfactory evidence that one of the interpretations is to be preferred over the others. The discrete-event simulation method just provides another description for the development of the outcomes of interference experiments. However, this does not mean that the simulation method tries to give an explanation of nature.

Structure

This thesis is structured as follows: In chapter 2, we discuss the discrete-event simulation method and the implementation of particles, optical elements, and devices applied in the simulations that we examine in the following chapters.

In chapter 3, we study a proposal for factoring numbers by using a network of Mach-Zehnder interferometers. We start with the basic idea and then consider two versions for the parallelization.

In chapter 4, we discuss briefly the random walk, followed by a study of the quantum random walk. We examine an experiment analytically and then apply the discrete-event simulation to see whether the method can be used to reproduce the distribution of the quantum random walk. Furthermore, we investigate an experiment where the quantum random walk is used to demonstrate a violation of the Leggett-Garg inequality.

Chapter 5 deals with the topic cryptography. Although we give an overview of the currently used non-quantum cryptosystems, our focus is on quantum key distribution. A discussion of the first quantum key distribution protocol is followed by a review of the current progress, especially regarding the security of (imperfect) implementations. Finally, we simulate a quantum key distribution experiment by means of the discrete-event simulation method.

In chapter 6, we first study the Franson-interferometer experiment analytically. Subsequently, we apply the discrete-event simulation approach to see whether we can reproduce the strong correlations observed in the experiment.

Finally, in the last chapter we give a summary of the topics we have covered and experiments that we have simulated. We also summarize briefly the discussions of and conclusions from all our obtained results.

2 Discrete-Event Simulations

Discrete-event simulations of quantum (optics) experiments [9] [10] [11] [12] [13] [14] [15] [16] are different from conventional simulation methods used for simulations of quantum phenomena in the sense that the Schrödinger equation does not need to be solved. In fact, not even a wave equation needs to be solved. Nevertheless, the method is capable of reproducing for example interference patterns observed in an interferometer experiment. The interference pattern is generated spot-by-spot, i.e., single particles are simulated which travel through an experimental setup and produce the interference pattern when being detected. The interference pattern builds up event-by-event without direct communication between the simulated particles. In fact, there is always only one particle in the setup, thus the only communication is due to a learning process of (some of) the devices depending on the internal state of the traveling particles.

This method can reproduce interference results predicted by quantum theory. As quantum theory gives predictions for averages only and not for single events, it is sufficient that the learning process of the (polarizing) beam splitters and detectors, which are the devices present in an interferometer, reproduces the correct frequencies. There is no need to justify changes in the states of the particles as quantum theory cannot describe what happens with the particle between preparation and detection.

An additional important fact about the discrete-event simulation method is that it only makes use of "locally causal, adaptive, classical dynamical systems" [14] and thus satisfies Einstein's criteria of realism and causality [9].

2.1 Random Numbers

Random numbers are a convenient, but not essential, ingredient of discrete-event simulations. However, true random numbers, i.e., numbers that originate in random statistical processes such as coin tosses, noise fluctuations, radioactive decays or the like and that cannot be predicted by anyone [17] are hard to obtain or take a long time to be generated. For simulation purposes, numbers that can be generated fast and appear to be random are usually sufficient. So we can draw on pseudo-random numbers which are generated deterministically by a pseudo-random number generator (PRNG). These numbers look random, i.e., the resulting sequence of pseudo-random numbers is indistinguishable from a true random number sequence for someone who does not know which algorithm has been used [17]. For this purpose, the algorithm of the PRNG has to fulfill some criteria such as the period of repetition has to be longer than the sequence of generated numbers. Depending on the application, some other criteria may also be required [17].

Since the PRNG is deterministic, it generates the same numbers each time it is started. To avoid that the PRNG generates the same numbers for every run of the program, it is possible to pass some initialization number, the so-called seed, to the PRNG. For different seeds, the sets of pseudo-random numbers generated by the PRNG are different. Nevertheless, using the same seed gives the same pseudo-random numbers which can be

useful, e.g., for debugging. So when we speak about random numbers in the context of simulations, these are usually pseudo-random numbers. However, note that many PRNGs that are sufficient for simulation purposes (such as e.g. the Mersenne Twister [18]) are not sufficient for cryptographic purposes. If pseudo-random numbers instead of true random numbers are used for cryptographic purposes, they have to be generated from a cryptographically secure PRNG such as for example the Blum-Blum-Shub generator [19].

2.2 Photons

For discrete-event simulations of (quantum) optics experiments, the simulated particles are photons which are described by a phase (just as classical light waves) and a polarization. The information called message and carried by the photon, also called messenger, can therefore be stored as a two-dimensional complex vector $\mathbf{m}$ of norm one

$$\mathbf{m} = \begin{pmatrix} \sin\xi\,(\cos\psi_1 + i\sin\psi_1) \\ \cos\xi\,(\cos\psi_2 + i\sin\psi_2) \end{pmatrix}, \tag{2.1}$$

where the two components are used to represent the polarization (e.g. vertical and horizontal) and are controlled by the parameters ξ, ψ_1, and ψ_2 [14]. The phases of the two polarization directions can be different, so they are stored in the complex numbers $\cos\psi_1 + i\sin\psi_1$ and $\cos\psi_2 + i\sin\psi_2$. Optical elements can change the parameters ξ, ψ_1, and ψ_2 and act differently depending on the message $\mathbf{m}$.

Moreover, in the simulation, the path of the photon is always well-defined and can be stored at arbitrary stages without disturbing the subsequent evolution.

In principle, the phases of the photons change in time just because the photons travel in space. If the photon's frequency is given by f, the phase changes in a time period Δt from ψ_i to $\psi_i + 2\pi f\Delta t$. Since only differences in the phases of different photons are relevant, the change of a phase is not taken into account if it affects all photons in the same way.

2.3 Sources

We usually consider single-photon sources such that the photons are emitted one by one. The sources are monochromatic, i.e., the frequencies of all photons leaving the source are the same.

However, there are cases (see section (5.2.3)) where we consider sources emitting photons with a frequency $f + \nu$ where f is fixed and ν is a Gaussian distributed random number where σ^2 is the variance:

$$p(\nu) = \frac{1}{\sqrt{2\pi}\sigma} e^{-\nu^2/(2\sigma^2)}. \tag{2.2}$$

The source emits always a number of N_ν photons with the same ν. Then a new ν is picked and N_ν photons leave the source with the new frequency $f + \nu$ and so on. This method is used when time itself and not only the phase of the photons is required. Due to the fluctuations in the frequencies, different path lengths for example in an unbalanced Mach-Zehnder interferometer (which will be introduced in chapter 5) can be considered in the sense that they do not only produce a phase shift, as they would when using the

simple model, but they lead to decoherence which appears in unbalanced Mach-Zehnder interferometers due to the time delay induced in only one of the interferometer arms.

For the Franson-interferometer experiment (see section 6.2), we use a two-photon source. This source emits two photons at once flying in opposite directions. The frequencies of the photons are $f \pm \nu$ such that the sum of them is constantly $2f$ and ν is distributed according to Eq. (2.2). In real experiments, usually parametric down-conversion is used where $2f$ would then be the frequency of the pump laser. Experiments like this, where we want to measure correlations, are the only ones where more than one photon, namely two photons, are in the setup at the same time. Nevertheless, these photons do neither communicate with each other directly nor through the optical devices as each travels through its own part of the experimental setup.

2.4 Phase Shifters and Wave Plates

Phase shifters and wave plates affect the message of a photon independently of its information carried, and therefore they are quite simple devices. A phase shifter which shifts the phase of a photon by φ, changes the incoming message $\mathbf{m}$ to

$$\mathbf{m}' = \begin{pmatrix} \sin\xi\,(\cos(\psi_1+\varphi) + i\sin(\psi_1+\varphi)) \\ \cos\xi\,(\cos(\psi_2+\varphi) + i\sin(\psi_2+\varphi)) \end{pmatrix}. \tag{2.3}$$

This can be achieved by multiplying the vector $\mathbf{m}$ with $\cos\varphi + i\sin\varphi$.

The wave plates are a bit more sophisticated as they also change the polarization included in the message. The action of the half-wave plate on the photon can be realized by multiplying the vector $\mathbf{m}$ with the matrix [14]

$$T_{\mathrm{HWP}}(\vartheta) = -i \begin{pmatrix} \cos 2\vartheta & \sin 2\vartheta \\ \sin 2\vartheta & -\cos 2\vartheta \end{pmatrix}, \tag{2.4}$$

where ϑ indicates the orientation of the optical axis. Considering the polarization states $|V\rangle$ (vertical polarization) and $|H\rangle$ (horizontal polarization), we get for $\vartheta = \pi/8$ the map $|V\rangle \mapsto -i(|V\rangle + |H\rangle)/\sqrt{2}$, $|H\rangle \mapsto -i(|V\rangle - |H\rangle)/\sqrt{2}$ which is proportional to the Hadamard-transformation on the polarization. In order to apply a Hadamard transformation, which is effectively a rotation of the polarization by $\pi/4$, we apply $T_{\mathrm{HWP}}(\pi/8)$ to the message followed by a phase shift by $\pi/2$, i.e., a multiplication with i. In total, the applied transformation is given by

$$H = i \cdot T_{\mathrm{HWP}}\left(\frac{\pi}{8}\right) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{2.5}$$

The flight through a quarter-wave plate can also be modeled by a matrix-vector multiplication with the matrix [14]

$$T_{\mathrm{QWP}}(\vartheta) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 - i\cos 2\vartheta & -i\sin 2\vartheta \\ -i\sin 2\vartheta & 1 + i\cos 2\vartheta \end{pmatrix}, \tag{2.6}$$

where ϑ again gives the orientation of the optical axis.

The implementation of these three devices in the discrete-event simulation is simply done by multiplying the message $\mathbf{m}$ by $\cos\varphi + i\sin\varphi$ to achieve a phase shift by φ, or by multiplying the matrices T_{HWP} or T_{QWP} with the vector $\mathbf{m}$ to apply a wave plate.

2.5 Beam Splitters

Now we investigate the functionality of a beam splitter. From quantum optics (see for example Ref. [20]) we know that a beam splitter acts on two incoming modes, say a and a', such that the output modes b and b' are given by

$$\begin{pmatrix} b \\ b' \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix} \begin{pmatrix} a \\ a' \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} a + ia' \\ ia + a' \end{pmatrix}. \tag{2.7}$$

If we additionally have vertical and horizontal polarization in each mode ($\mathbf{a} = (a_v,\ a_h)^T$), the transformation-matrix is given by

$$T_{\mathrm{BS}} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i & 0 & 0 \\ i & 1 & 0 & 0 \\ 0 & 0 & 1 & i \\ 0 & 0 & i & 1 \end{pmatrix}, \tag{2.8}$$

if the two incoming modes are put into a vector as follows:

$$\begin{pmatrix} a_v \\ a'_v \\ a_h \\ a'_h \end{pmatrix}.$$

A sketch showing where each of the modes enters or leaves the beam splitter is depicted in Fig. 2.1. The matrix of the beam splitter acts actually on the horizontally and vertically polarized parts independently as horizontally and vertically polarized photons do not interfere because of being distinguishable by their different polarizations.

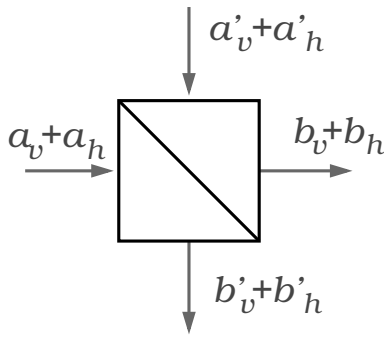

Figure 2.1: Sketch of a beam splitter. The white square with the diagonal line depicts the beam splitter, gray arrows visualize incoming and outgoing modes. Incoming modes are denoted by a_i and a'_i where $i = v, h$, and b_i and b'_i indicate outgoing modes.

However, for the discrete-event simulation this transformation-matrix is not sufficient as there is only one photon at a time allowed to be in the experimental setup. Therefore, the photon has to be in either mode $\mathbf{a}$ or $\mathbf{a}'$ before it enters the beam splitter, but it also has to be in either mode $\mathbf{b}$ or $\mathbf{b}'$ after it leaves the beam splitter. For this purpose, a mechanism that decides in which mode the photon leaves the beam splitter when it enters in mode $\mathbf{a}$ or $\mathbf{a}'$ is needed. We use the stochastic learning machine (which is also described in Refs. [9] [14] [16]) which "remembers" the messages carried by the photons

entering in the two modes. The probability at which port the actual photon leaves the beam splitter, and which message it carries, depends partly on the messages and input ports of the previous photons and the current photon. After a sufficient number of photons has passed through the beam splitter, this probability converges to the probability also expected for the interference pattern if photons enter at both input ports, for example at the second beam splitter of a Mach-Zehner interferometer.

How does this machine work in detail? The beam splitter can store two complex unit vectors $\mathbf{Y}_0$ and $\mathbf{Y}_1$ of dimension two, and two real valued numbers x_0 and x_1 which fulfill $x_0, x_1 \geq 0$ and $x_0 + x_1 = 1$. All of these numbers are initialized randomly. The vector $\mathbf{Y}_0$ or $\mathbf{Y}_1$ is updated when a photon enters through port 0 or 1, respectively. If the photon enters port i, $\mathbf{Y}_i$ is then set to the message carried by this photon. x_0 and x_1 are updated via the rule

$$x_i \leftarrow \gamma x_i + (1 - \gamma) \tag{2.9}$$

$$x_j \leftarrow \gamma x_j, \tag{2.10}$$

where i is the port the photon enters, j is the other one, and $\gamma \in [0, 1)$ is a parameter to control the "learning process" and which we usually choose to be $\gamma = 0.98$. In chapter 6, we use $\gamma = 0.6$ (Ref. [9] includes discussions with different γ). This rule leads to x_0 and x_1 containing the frequency at which the photons arrive at the two ports after sufficiently many have passed the beam splitter.

The numbers x_0 and x_1 are used to adjust the stored messages according to their frequencies as follows:

$$\begin{pmatrix} Y'_{0,v} \\ Y'_{1,v} \\ Y'_{0,h} \\ Y'_{1,h} \end{pmatrix} = \begin{pmatrix} \sqrt{x_0} & 0 & 0 & 0 \\ 0 & \sqrt{x_1} & 0 & 0 \\ 0 & 0 & \sqrt{x_0} & 0 \\ 0 & 0 & 0 & \sqrt{x_1} \end{pmatrix} \begin{pmatrix} Y_{0,v} \\ Y_{1,v} \\ Y_{0,h} \\ Y_{1,h} \end{pmatrix}, \tag{2.11}$$

where $Y_{i,v}$ ($Y_{i,h}$) denotes the vertical (horizontal) component of the message last registered at port i. $\mathbf{Y}'_i$ are temporary vectors containing the modified messages. This modification leads then to the correct weighting of the messages. The reason for this is that the messages are always normalized, but for the beam splitter, the superposition has to be normalized with in general two different weights for the summands. So if the particles enter for example only at port i, the random initialization of the other vector is not relevant since x_i converges to one, and the other one to zero. After the modification of the vectors $\mathbf{Y}_0$ and $\mathbf{Y}_1$, the actual beam splitter transformation is applied, and we obtain

$$\begin{pmatrix} W_{0,v} \\ W_{1,v} \\ W_{0,h} \\ W_{1,h} \end{pmatrix} := T_{\mathrm{BS}} \begin{pmatrix} Y'_{0,v} \\ Y'_{1,v} \\ Y'_{0,h} \\ Y'_{1,h} \end{pmatrix}. \tag{2.12}$$

We have $|W_{0,v}|^2 + |W_{0,h}|^2 + |W_{1,v}|^2 + |W_{1,h}|^2 = 1$ since $|Y'_{0,v}|^2 + |Y'_{1,v}|^2 + |Y'_{0,h}|^2 + |Y'_{1,h}|^2 = 1$ and T_{BS} is unitary. A (pseudo) random number $r \in [0, 1]$ is then used to decide through which port the photon leaves the beam splitter. This decision depends on $w_0 := |W_{0,v}|^2 + |W_{0,h}|^2 \in [0, 1]$ in the following way: If $r < w_0$, the photon leaves through port 0, and if $r \geq w_0$, the photon leaves through port 1. The message the photon carries when it leaves

the beam splitter at port i is set to

$$\mathbf{m}' = \frac{1}{\sqrt{|W_{i,v}|^2 + |W_{i,h}|^2}} \begin{pmatrix} W_{i,v} \\ W_{i,h} \end{pmatrix}. \tag{2.13}$$

The message $\mathbf{m}'$ is again normalized such that the photon carries in the end a message with norm one.

The result is the same when using a dielectric plate to model the beam splitter instead of directly using the transformation matrix T_{BS} [13].

In the case of incoherent light, for example in the case of a source with fluctuating frequency, there is no interference in the beam splitter. Then we can replace the beam splitter with learning machine by a simple comparison of a uniformly distributed random number $r \in [0, 1]$ with 0.5. If $r > 0.5$, the output port is 0, otherwise it is 1. If the photon was reflected, i.e., if the number of the input port does not equal the number of the output port, a phase shift of $\pi/2$ is applied.

2.5.1 Polarizing Beam Splitters

For simulating the polarizing beam splitter, we employ the stochastic learning machine which we also used to achieve the expected behavior of the common beam splitter. Thus, the polarizing beam splitter also has two complex, two-dimensional vectors $\mathbf{Y}_0$ and $\mathbf{Y}_1$, two real-valued positive numbers x_0 and x_1 which sum up to one, and the fixed learning parameter γ that is usually set to $\gamma = 0.98$. The update rules for the x_i and $\mathbf{Y}_i$, $i \in \{0, 1\}$, are the same as before: Depending on the input port, x_0 and x_1 are updated according to Eqs. (2.9) and (2.10) where i is the port on which the message arrives and j is the other one. The vectors $\mathbf{Y}_0$ and $\mathbf{Y}_1$ are updated according to Eq. (2.11). The only change is that instead of T_{BS}, we use the transformation-matrix of the polarizing beam splitter given by [14]

$$T_{\mathrm{PBS}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & i \\ 0 & 0 & i & 0 \end{pmatrix}, \tag{2.14}$$

to compute the temporal vectors $\mathbf{W}_0$ and $\mathbf{W}_1$ as given in Eq. (2.13). Which output port is chosen and which message leaves the polarizing beam splitter is determined in the same way as for the common beam splitter by comparison of the norm of $\mathbf{W}_0$ with a random number.

Using this kind of transformation for the polarizing beam splitter, vertically polarized photons will be transmitted and horizontally polarized photons will be reflected in a statistical manner. Since quantum theory gives only information about averages, it is sufficient that the stochastic learning machine just reproduces the frequencies expected from quantum theory and does not necessarily transmit or reflect each single photon according to its polarization.

2.6 Detectors

We consider two different kinds of detectors from which we choose one kind depending on the experiment. The simple detector only counts arriving photons, so an integer as a

counter is already sufficient. For more than only one detector, an array with an entry for each detector is convenient.

This simple version, however, does not work for all experiments. So sometimes we have to use a more sophisticated approach which would always work but often makes things more complex than necessary. For this more sophisticated detector, we also use a learning machine. This type of detector is also used in Refs. [12] and [15]. The detector can store two complex numbers Y_v and Y_h which are initialized at random and then updated according to the rule

$$Y_i \leftarrow \gamma Y_i + (1-\gamma) m_i \tag{2.15}$$

for each incoming message $\mathbf{m} = (m_v, m_h)^T$ and $i \in \{v, h\}$. The detector only clicks if uniformly distributed random numbers $r_1, r_2 \in [0, 1]$ generated anew for each event fulfill $r_1 < |Y_v|^2 + |Y_h|^2$ and $r_2 < \eta$, where η is the desired detection efficiency of the detector.

3 Factoring With Mach-Zehnder Interferometers

Shor's algorithm for factoring numbers on a quantum computer achieves an exponential speedup compared to factoring on a classical computer such that the factoring problem could in principle be solved in polynomial time [21]. Summhammer proposed a factoring algorithm which makes use only of Mach-Zehnder interferometers and photodetectors [22]. Although the speedup is not exponential for this algorithm, it has the advantage that instead of a quantum computer only a network of Mach-Zehnder interferometers is needed.

In this chapter, we will investigate this proposal and apply the discrete-event simulation to the setup of Mach-Zehnder interferometers in order to first get used to the discrete-event simulation as here we only need phase shifters and beam splitters, and second, to see whether this implementation might be a step towards an efficient way of factoring large numbers.

3.1 Investigation of the Basic Idea

First, we have a look at the basic idea of Summhammer's proposal [22]. The setup is shown in Fig. 3.1. Basically, the setup consists of Mach-Zehnder interferometers placed one after another. As in the proposal [22], we examine up to three successive interferometers.

The main idea is that simultaneously increasing the phase differences in the Mach-Zehnder interferometers in discrete steps and summing up the intensities at the detectors leads to different intensity patterns depending on the step width. A clever choice of the step width can be used to determine factors of an integer N. If the phase χ_i of the phase shifter contained in the i-th Mach-Zehnder interferometer is increased in steps of $2\pi/n_i$, where $n_i < n_j$ for $1 \leq i < j \leq 7$ and $n_i \in \mathbb{N}$, then the n_i can be tested for being factors of N. For that, the intensities at the detectors have to be registered every N increments only. After l increases we have $\chi_i(l) = 2\pi l/n_i$ for all i, but we are only interested in the intensities after $l = N, 2N, 3N, \ldots, n_7 N$ increments. So the idea of the proposal is that if some of the n_i are factors of N, which is to be factorized, it is possible to determine which ones of the n_i are factors by measuring the intensity pattern at the detectors.

We first have a look at one interferometer only (Fig. 3.2) with ideal detectors (i.e. the detection efficiency is 100%). The probability that a photon is detected at the upper detector, which we labeled by A, is

$$p_A(\chi(l)) = \frac{1}{2}\left(1 + \cos\chi(l)\right). \tag{3.1}$$

For $l = kN$, we find for the probability

$$p_A(\chi(kN)) = \frac{1}{2}\left(1 + \cos\left(\frac{2\pi kN}{n}\right)\right), \tag{3.2}$$

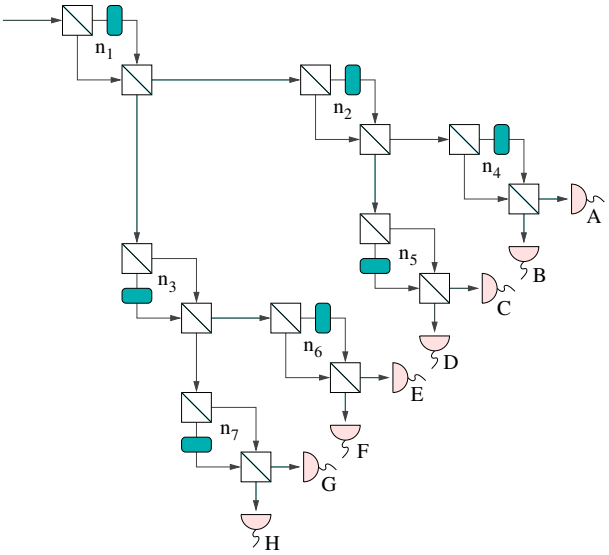

Figure 3.1: Setup of Mach-Zehnder interferometers for the factoring algorithm proposed in Ref. [22] by Summhammer. White boxes with a diagonal line represent 50:50 beam splitters, cyan ellipses denote phase shifters where n_i with $i = 1, \ldots, 7$ indicate that the phase shifter can be incremented in steps of $2\pi/n_i$. Pink half-circles with a wiggly line denote detectors labeled by A, B, $\ldots$, H.

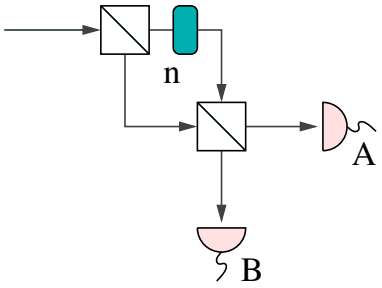

Figure 3.2: A single Mach-Zehnder interferometer as part of the setup given in Fig. 3.1 with the same meanings of the symbols.

which is 1 if n is a factor of N. Adding up the probabilities to measure photons at detector A for $k = 1, \ldots, n$ we obtain the intensity

$$I = \sum_{k=1}^{n} p_A(\chi(kN)) = \frac{n}{2} + \frac{1}{2}\sum_{k=1}^{n} \cos\left(\frac{2\pi kN}{n}\right). \tag{3.3}$$

If n is a factor of N, $I = n$ and otherwise $I \approx n/2$ because the summation over k of $\cos(2\pi kN/n)$ averages approximately to zero as stated in [22].

Taking into account the interferometers 1, 2, and 4 as labeled in Fig. 3.3, we have to sum from $k = 1$ to $k = n_4$ as n_4 is the largest denominator occurring in one of the cosines. To obtain the intensity at detector A we have to multiply the probabilities that the photons leave the interferometers in the upper direction, and perform the sum over k [22]:

$$I_A = \frac{1}{8}\sum_{k=1}^{n_4}\left(1+\cos\left(\frac{2\pi kN}{n_1}\right)\right)\left(1+\cos\left(\frac{2\pi kN}{n_2}\right)\right)\left(1+\cos\left(\frac{2\pi kN}{n_4}\right)\right). \tag{3.4}$$

The intensities at the other detectors result from multiplying the probabilities of the outputs directing to the corresponding detectors:

$$I_B = \frac{1}{8}\sum_{k=1}^{n_4}\left(1+\cos\left(\frac{2\pi kN}{n_1}\right)\right)\left(1+\cos\left(\frac{2\pi kN}{n_2}\right)\right)\left(1-\cos\left(\frac{2\pi kN}{n_4}\right)\right) \tag{3.5}$$

$$I_{C+D} = \frac{1}{8}\sum_{k=1}^{n_4}\left(1+\cos\left(\frac{2\pi kN}{n_1}\right)\right)\left(1-\cos\left(\frac{2\pi kN}{n_2}\right)\right) \tag{3.6}$$

$$I_{E+F+G+H} = \frac{1}{8}\sum_{k=1}^{n_4}\left(1-\cos\left(\frac{2\pi kN}{n_1}\right)\right). \tag{3.7}$$

Since we register the intensities only every N increments, we can enlarge the increments by a factor of N which speeds up the computation.

In the simulation, for each increment we generate $L = 10\,000$ messengers with random polarization and initial phase. The messengers then pass a Mach-Zehnder interferometer and depending on the output direction, they are detected or sent to the next Mach-Zehnder interferometer as depicted in Fig. 3.3. A Mach-Zehnder interferometer is composed of two beam splitters where in between a phase shifter is inserted in one of the arms as represented in Fig. 3.2. The phase shifters and beam splitters are implemented as described in section 2.4 and 2.5, respectively. After maximally three Mach-Zehnder interferometers, the messengers are detected which means they simply lead to an increment of the counter of the corresponding detector. The normalized intensities are obtained by dividing these counters by Ln_4.

The expected intensities at the detectors A to H, using the argumentation presented in Ref. [22], are given in Table 3.1 for different combinations of n_1, n_2, and n_4 being factors of N. All possible outcomes are unique such that the factors can be extracted unambiguously. The numerical evaluation of the sums occurring in the analytical expressions of the intensities are shown in Table 3.2 together with the results of the discrete-event simulation for various N, n_1, n_2, and n_4.

Table 3.1: Expected intensities at the detectors A to H depending on whether n_1, n_2, and n_4 are factors or nonfactors of N. "F" indicates a factor of N and "$-$" indicates a nonfactor. To allow for direct comparison with Table 3.2, the intensities are divided by n_4 such that they are normalized and sum up to 1. This table is also given in Ref. [22].

n_1	n_2	n_4	I_A	I_B	I_{C+D}	$I_{E+F+G+H}$
F	F	F	1	0	0	0
F	F	–	0.5	0.5	0	0
F	–	F	0.5	0	0.5	0
F	–	–	0.25	0.25	0.5	0
–	F	F	0.5	0	0	0.5
–	F	–	0.25	0.25	0	0.5
–	–	F	0.25	0	0.25	0.5
–	–	–	0.125	0.125	0.25	0.5

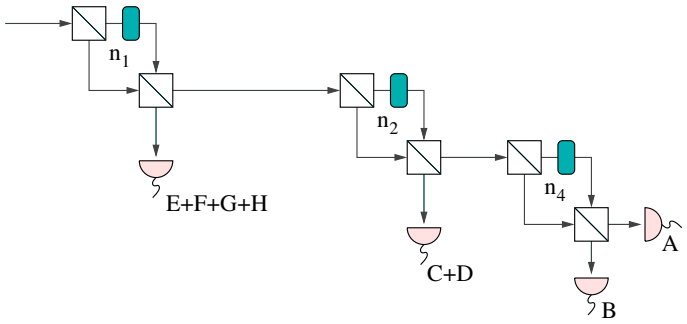

Figure 3.3: Upper part of the setup shown in Fig. 3.1 as it is used in the first part of the simulation. The symbols have the same meaning as in Fig. 3.1. The detector labels $C+D$ and $E+F+G+H$ indicate which detectors are consolidated and replaced by only one detector.

Table 3.2: Normalized intensities measured in the discrete-event simulation and Eqs. (3.4) - (3.7) numerically evaluated for various N, n_1, n_2, and n_4, rounded to four decimals. Red numbers are factors of N.

				Simulation				Numerical Summation			
N	n_1	n_2	n_4	I_A	I_B	I_{C+D}	$I_{E+F+G+H}$	I_A	I_B	I_{C+D}	$I_{E+F+G+H}$
30	2	3	5	0.989	0.003	0.003	0.004	1	0	0	0
385	5	7	11	0.991	0.003	0.003	0.003	1	0	0	0
1001	7	11	13	0.991	0.003	0.003	0.003	1	0	0	0
23161	19	23	53	0.992	0.003	0.003	0.003	1	0	0	0
6	2	3	5	0.494	0.499	0.003	0.004	0.5	0.5	0	0
35	5	7	11	0.495	0.499	0.003	0.003	0.5	0.5	0	0
77	7	11	13	0.496	0.498	0.003	0.003	0.5	0.5	0	0
23161	19	23	29	0.498	0.497	0.003	0.003	0.5	0.5	0	0
10	2	3	5	0.394	0.002	0.600	0.004	0.4	0	0.6	0
55	5	7	11	0.433	0.002	0.562	0.003	0.436	0	0.564	0
91	7	11	13	0.455	0.002	0.540	0.003	0.458	0	0.542	0
23161	19	29	53	0.493	0.002	0.502	0.003	0.497	0	0.503	0
14	2	3	5	0.137	0.262	0.598	0.004	0.139	0.261	0.6	0
25	5	7	11	0.214	0.252	0.531	0.003	0.213	0.254	0.533	0
49	7	11	13	0.243	0.249	0.504	0.003	0.245	0.251	0.505	0
23161	19	29	47	0.249	0.248	0.501	0.003	0.250	0.249	0.501	0
15	2	3	5	0.397	0.002	0.003	0.598	0.4	0	0	0.6
77	5	7	11	0.459	0.002	0.002	0.537	0.463	0	0	0.537
143	7	11	13	0.458	0.002	0.002	0.539	0.462	0	0	0.534
23161	17	19	53	0.493	0.002	0.002	0.504	0.496	0	0	0.504
21	2	3	5	0.151	0.248	0.003	0.598	0.15	0.25	0	0.6
49	5	7	11	0.240	0.273	0.002	0.486	0.241	0.273	0	0.486
121	7	11	13	0.287	0.174	0.002	0.537	0.288	0.173	0	0.538
23161	17	23	47	0.242	0.249	0.002	0.507	0.243	0.250	0	0.507
35	2	3	5	0.098	0.001	0.303	0.598	0.1	0	0.3	0.6
121	5	7	11	0.243	0.001	0.270	0.485	0.244	0	0.270	0.486
169	7	11	13	0.199	0.001	0.260	0.539	0.201	0	0.261	0.538
23161	17	29	53	0.241	0.001	0.254	0.504	0.242	0	0.254	0.504
49	2	3	5	0.037	0.064	0.301	0.598	0.038	0.063	0.3	0.6
169	5	7	11	0.091	0.094	0.331	0.485	0.090	0.095	0.329	0.486
529	7	11	13	0.109	0.136	0.217	0.538	0.108	0.136	0.218	0.538
23161	17	31	47	0.119	0.126	0.247	0.507	0.119	0.126	0.247	0.507
190748	53	59	61	0.325	0.080	0.148	0.446	0.327	0.079	0.148	0.446

The results of the simulation fit nicely with the numerical evaluation of the summations. However, they do not always coincide with the expectations given in Ref. [22] and Table 3.1. Some results, for example these where n_1 and n_2 are factors of N, fit well. But especially the results for small n_i, where n_1 or n_2 is not a factor of N, deviate quite a lot from the expectations given in Table 3.1. But also results for larger n_i can be worse than for smaller ones (see last two rows of Table 3.2).

The deviations of the exact numerical evaluations of the sums from the results given in Ref. [22] and Table 3.1 show that the evaluations of the sums given in Eqs. (3.4) - (3.7) have to be done more carefully than in Ref. [22]. The deviations occur because the approximation

$$\sum_{k=1}^{n_i} \cos\left(\frac{2\pi k N}{n_j}\right) \approx 0, \qquad n_j \nmid N, \tag{3.8}$$

is not necessarily valid if $n_i \neq n_j$. So depending on N, n_i and n_j, this approximation can work but it may also lead to significant errors. Nevertheless, this setup is usually capable of indicating factors of N as Table 3.1 provides clear relations such that often even more severe deviations still lead to distinct assignments. However, unclear intensity patterns due to deviations that are too large can possibly lead to wrong identifications of factors. For example for $N = 190748$ in Table 3.2, the intensity pattern suggests that n_4 is a factor, but it is not. Only in comparison to the other results, we can see that when we expect zero intensity, the intensity is in all simulations and evaluations close to zero (≤ 0.004). An intensity of about 0.08 has to correspond to an expected intensity greater than zero. Taking this into account, we find that the best fitting intensity pattern corresponds to the case where none of the n_i, $i = 1, 2, 4$, is a factor of N, which is the correct case. Analyzing the results carefully, the correct pattern can be identified in all tested cases.

3.2 A Simple Extension

As the aim is a parallel test for factors of N, it is reasonable to also consider the intensities at the detectors C to H separately and thus take into account the interferometers 3, 5, 6, and 7 from Fig. 3.1. So it is possible to test all the numbers n_1 through n_7 for being factors of N. However, if one or more of these numbers are factors of N we may not be able to say whether we found all the factors, but at least one of them. If n_1, n_2 or n_3 is a factor of N, we are not able to say whether they are the only factors as some detectors will not detect any photons at all. For example if n_2 is a factor, we cannot say anything about n_5 since there will be no photons flying through the fifth interferometer.

The intensities at detectors A and B are the same as those already given in Eqs. (3.4)

and (3.5). At the other detectors, the intensities are given by

$$I_C = \frac{1}{8}\sum_{k=1}^{n_7}\left(1+\cos\left(\frac{2\pi kN}{n_1}\right)\right)\left(1-\cos\left(\frac{2\pi kN}{n_2}\right)\right)\left(1-\cos\left(\frac{2\pi kN}{n_5}\right)\right) \tag{3.9}$$

$$I_D = \frac{1}{8}\sum_{k=1}^{n_7}\left(1+\cos\left(\frac{2\pi kN}{n_1}\right)\right)\left(1-\cos\left(\frac{2\pi kN}{n_2}\right)\right)\left(1+\cos\left(\frac{2\pi kN}{n_5}\right)\right) \tag{3.10}$$

$$I_E = \frac{1}{8}\sum_{k=1}^{n_7}\left(1-\cos\left(\frac{2\pi kN}{n_1}\right)\right)\left(1-\cos\left(\frac{2\pi kN}{n_3}\right)\right)\left(1+\cos\left(\frac{2\pi kN}{n_6}\right)\right) \tag{3.11}$$

$$I_F = \frac{1}{8}\sum_{k=1}^{n_7}\left(1-\cos\left(\frac{2\pi kN}{n_1}\right)\right)\left(1-\cos\left(\frac{2\pi kN}{n_3}\right)\right)\left(1-\cos\left(\frac{2\pi kN}{n_6}\right)\right) \tag{3.12}$$

$$I_G = \frac{1}{8}\sum_{k=1}^{n_7}\left(1-\cos\left(\frac{2\pi kN}{n_1}\right)\right)\left(1+\cos\left(\frac{2\pi kN}{n_3}\right)\right)\left(1-\cos\left(\frac{2\pi kN}{n_7}\right)\right) \tag{3.13}$$

$$I_H = \frac{1}{8}\sum_{k=1}^{n_7}\left(1-\cos\left(\frac{2\pi kN}{n_1}\right)\right)\left(1+\cos\left(\frac{2\pi kN}{n_3}\right)\right)\left(1+\cos\left(\frac{2\pi kN}{n_7}\right)\right). \tag{3.14}$$

As in the previous case, it is sufficient to increment the phases χ_i by $2\pi N/n_i$ and thus speed up the computation. Therefore, in the simulation we consider $\chi_i = 2\pi kN/n_i$ for $k = 1, 2, \ldots, n_7$ only. Again we generate $L = 10\,000$ messengers for each increment with random initial phase and polarization. But in this version, each messenger passes through three Mach-Zehnder interferometers as depicted in Fig. 3.1. In the end, each messenger contributes to one of the eight counters corresponding to the detectors as we simulate ideal photodetectors. Dividing the counters by Ln_7 normalizes the intensities such they sum up to one.

The simulation results are given in Table 3.3 together with the numerical evaluations of the sums for the intensities. The results for $N = 115$ and $N = 325$ illustrate the before mentioned example, as n_2 is in both cases a factor but for $N = 325$, n_5 is also a factor. Yet still we get similar intensity patterns for both numbers. The expected intensities based on the approximation given in Eq. (3.8) are presented in Table 3.4. As before, these expected intensities are not achieved perfectly due to the approximation (3.8). However in this way, the intensity patterns given in Table 3.4 do not depend on the numbers n_i, $i = 1, 2, \ldots, 7$ and N, but they are good enough to compare with and identify at least one factor of N from the results presented in Table 3.3.

Thus, the simple extension is capable of finding at least one factor of N if at least one factor is contained within the n_i. However, there may be factors a single run cannot detect. So probably more than one run with different n_i is necessary to find all the factors of N. However, the nice feature of this procedure is that we only need n_7 increments simultaneously of all phases χ_i, $i = 1, 2, \ldots, 7$. Although approximations have been made, it is still possible to identify the correct intensity pattern and thus the corresponding factors.

In the next section, we will examine the more complex proposal for parallelization mentioned by Summhammer in Ref. [22].

Table 3.3: Simulation results of the simple implementation which possibly fails to find all factors. Given are N, n_i, $i = 1, 2, \ldots, 7$ and the intensities at the detectors A, B, $\ldots H$ achieved from the simulation (upper row) and from the numerical evaluation of the sums (lower row). The red numbers are factors of N. The results of the simulation and the numerical evaluation coincide well. The intensities are similar for $N = 115$ and $N = 325$ although for $N = 115$, n_5 is not a factor but for $N = 325$ it is.

N	n_1	n_2	n_3	n_4	n_5	n_6	n_7	I_A	I_B	I_C	I_D	I_E	I_F	I_G	I_H
529	3	5	7	11	13	17	19	0.082	0.139	0.137	0.129	0.135	0.104	0.135	0.139
								0.082	0.139	0.137	0.129	0.135	0.104	0.133	0.141
217	7	11	13	17	19	23	29	0.247	0.247	0.253	0.251	0.001	0.001	0.001	0.001
								0.247	0.247	0.255	0.251	0	0	0	0
345	3	5	7	11	13	17	19	0.491	0.503	0.001	0.001	0.001	0.001	0.001	0.001
								0.495	0.505	0	0	0	0	0	0
693	3	5	7	11	13	17	19	0.471	0.002	0.248	0.276	0.001	0.001	0.001	0.001
								0474	0	0.248	0.278	0	0	0	0
115	3	5	7	11	13	17	19	0.234	0.251	0.001	0.001	0.153	0.086	0.123	0.151
								0.236	0.251	0	0	0.153	0.086	0.123	0.152
325	3	5	7	11	13	17	19	0.234	0.251	0.001	0.001	0.135	0.105	0.153	0.120
								0.236	0.251	0	0	0.135	0.104	0.153	0.121
169	7	11	13	17	19	23	29	0.101	0.141	0.121	0.147	0.001	0.001	0.226	0.262
								0.100	0.141	0.122	0.148	0	0	0.226	0.263
299	7	11	13	17	19	23	29	0.109	0.137	0.141	0.108	0.001	0.001	0.219	0.284
								0.109	0.137	0.142	0.108	0	0	0.219	0.285
377	7	11	13	17	19	23	29	0.119	0.126	0.124	0.140	0.001	0.001	0.001	0.487
								0.119	0.126	0.124	0.141	0	0	0	0.489
323	7	11	13	17	19	23	29	0.241	0.001	0.001	0.267	0.162	0.137	0.143	0.047
								0.241	0	0	0.270	0.162	0.138	0.144	0.046

Table 3.4: Relations between the n_i, $i = 1, 2, \ldots, 7$, being factors ("F") or nonfactors ("−") and the corresponding expected intensities in the detectors $A, ..., H$. A questionmark ("?") denotes that the respective n_i does not affect the intensities, i.e., one cannot tell from the measured intensities whether n_i is a factor of N or whether it is not. Although this procedure does not give enough information to find all possible factors, it can still be used to identify some factors of N.

n_1	n_2	n_3	n_4	n_5	n_6	n_7	I_A	I_B	I_C	I_D	I_E	I_F	I_G	I_H
-	-	-	-	-	-	-	0.125	0.125	0.125	0.125	0.125	0.125	0.125	0.125
-	-	-	-	F	-	-	0.125	0.125	0	0.25	0.125	0.125	0.125	0.125
-	-	F	-	-	?	-	0.125	0.125	0.125	0.125	0	0	0.25	0.25
-	-	-	-	-	-	F	0.125	0.125	0.125	0.125	0.125	0.125	0	0.25
-	-	-	-	-	F	-	0.125	0.125	0.125	0.125	0.25	0	0.125	0.125
-	-	-	F	-	-	-	0.25	0	0.125	0.125	0.125	0.125	0.125	0.125
-	F	-	-	?	-	-	0.25	0.25	0	0	0.125	0.125	0.125	0.125
F	-	?	-	-	?	?	0.25	0.25	0.25	0.25	0	0	0	0
-	-	F	-	F	?	-	0.125	0.125	0	0.25	0	0	0.25	0.25
-	-	-	-	F	-	F	0.125	0.125	0	0.25	0.125	0.125	0	0.25
-	-	-	-	F	F	-	0.125	0.125	0	0.25	0.25	0	0.125	0.125
-	-	F	-	-	?	F	0.125	0.125	0.125	0.125	0	0	0	0.5
-	-	-	-	-	F	F	0.125	0.125	0.125	0.125	0.25	0	0	0.25
-	-	-	F	F	-	-	0.25	0	0	0.25	0.125	0.125	0.125	0.125
-	-	F	F	-	?	-	0.25	0	0.125	0.125	0	0	0.25	0.25
-	-	-	F	-	-	F	0.25	0	0.125	0.125	0.125	0.125	0	0.25
-	-	-	F	-	F	-	0.25	0	0.125	0.125	0.25	0	0.125	0.125
-	F	F	-	?	?	-	0.25	0.25	0	0	0	0	0.25	0.25
-	F	-	-	?	-	F	0.25	0.25	0	0	0.125	0.125	0	0.25
-	F	-	-	?	F	-	0.25	0.25	0	0	0.25	0	0.125	0.125
F	-	?	-	F	?	?	0.25	0.25	0	0.5	0	0	0	0
-	F	-	F	?	-	-	0.5	0	0	0	0.125	0.125	0.125	0.125
F	-	?	F	-	?	?	0.5	0	0.25	0.25	0	0	0	0
F	F	?	-	?	?	?	0.5	0.5	0	0	0	0	0	0
-	-	F	-	F	?	F	0.125	0.125	0	0.25	0	0	0	0.5
-	-	-	-	F	F	F	0.125	0.125	0	0.25	0.25	0	0	0.25
-	-	F	F	F	?	-	0.25	0	0	0.25	0	0	0.25	0.25
-	-	-	F	F	-	F	0.25	0	0	0.25	0.125	0.125	0	0.25
-	-	-	F	F	F	-	0.25	0	0	0.25	0.25	0	0.125	0.125
-	-	F	F	-	?	F	0.25	0	0.125	0.125	0	0	0	0.5
-	-	-	F	-	F	F	0.25	0	0.125	0.125	0.25	0	0	0.25
-	F	F	-	?	?	F	0.25	0.25	0	0	0	0	0	0.5
-	F	-	-	?	F	F	0.25	0.25	0	0	0.25	0	0	0.25
-	F	F	F	?	?	-	0.5	0	0	0	0	0	0.25	0.25
-	F	-	F	?	-	F	0.5	0	0	0	0.125	0.125	0	0.25
-	F	-	F	?	F	-	0.5	0	0	0	0.25	0	0.125	0.125
F	-	?	F	F	?	?	0.5	0	0	0.5	0	0	0	0
F	F	?	F	?	?	?	1	0	0	0	0	0	0	0
-	-	F	F	F	?	F	0.25	0	0	0.25	0	0	0	0.5
-	-	-	F	F	F	F	0.25	0	0	0.25	0.25	0	0	0.25
-	F	F	F	?	?	F	0.5	0	0	0	0	0	0	0.5
-	F	-	F	?	F	F	0.5	0	0	0	0.25	0	0	0.25

3.3 The Actual Proposal for Parallelization

If we want to find only one factor of N, the procedure discussed in the previous section is already sufficient. But if we want to find all the factors, the summations of the probabilities for the detectors C through H have to be modified such that the probability of detecting a photon can be unequal to zero even if n_1, n_2 or n_3 is a factor of N. To test whether n_3 or n_7 are factors of N, Summhammer proposes to wait for about $n_1/2$ increments of χ_1, and then start incrementing χ_3 and χ_7 [22]. So at detector H the measured intensity is

$$\begin{aligned} I_H &= \frac{1}{8}\sum_{k=1}^{n_7}\left(1-\cos\left(\frac{2\pi(kN+n_1/2)}{n_1}\right)\right)\left(1+\cos\left(\frac{2\pi kN}{n_3}\right)\right)\left(1+\cos\left(\frac{2\pi kN}{n_7}\right)\right) \\ &\approx \frac{1}{8}\sum_{k=1}^{n_7}\left(1-\cos\left(\frac{2\pi kN}{n_1}+\pi\right)\right)\left(1+\cos\left(\frac{2\pi kN}{n_3}\right)\right)\left(1+\cos\left(\frac{2\pi kN}{n_7}\right)\right) \\ &= \frac{1}{8}\sum_{k=1}^{n_7}\left(1+\cos\left(\frac{2\pi kN}{n_1}\right)\right)\left(1+\cos\left(\frac{2\pi kN}{n_3}\right)\right)\left(1+\cos\left(\frac{2\pi kN}{n_7}\right)\right), \end{aligned} \tag{3.15}$$

and accordingly for detector G

$$\begin{aligned} I_G &= \frac{1}{8}\sum_{k=1}^{n_7}\left(1-\cos\left(\frac{2\pi(kN+n_1/2)}{n_1}\right)\right)\left(1+\cos\left(\frac{2\pi kN}{n_3}\right)\right)\left(1-\cos\left(\frac{2\pi kN}{n_7}\right)\right) \\ &\approx \frac{1}{8}\sum_{k=1}^{n_7}\left(1+\cos\left(\frac{2\pi kN}{n_1}\right)\right)\left(1+\cos\left(\frac{2\pi kN}{n_3}\right)\right)\left(1-\cos\left(\frac{2\pi kN}{n_7}\right)\right), \end{aligned} \tag{3.16}$$

where the approximations can be made if $2\cdot\lfloor n_1/2\rfloor \approx n_1$. Then we achieve a similar table for the output of the detectors H and G as we have for detectors A and B [22].

To test whether n_5 is a factor of N, we have to proceed similarly: We start incrementing the phases χ_1 and χ_2, wait for about $n_2/2$ steps and then start incrementing the phase χ_5. The intensity at detector D is then given by

$$\begin{aligned} I_D &= \frac{1}{8}\sum_{k=1}^{n_7}\left(1+\cos\left(\frac{2\pi(kN+n_2/2)}{n_1}\right)\right)\left(1-\cos\left(\frac{2\pi(kN+n_2/2)}{n_2}\right)\right)\left(1+\cos\left(\frac{2\pi kN}{n_5}\right)\right) \\ &\approx \frac{1}{8}\sum_{k=1}^{n_7}\left(1+\cos\left(\frac{2\pi kN}{n_1}+\pi\frac{n_2}{n_1}\right)\right)\left(1-\cos\left(\frac{2\pi kN}{n_2}+\pi\right)\right)\left(1+\cos\left(\frac{2\pi kN}{n_5}\right)\right) \\ &= \frac{1}{8}\sum_{k=1}^{n_7}\left(1+\cos\left(\frac{2\pi kN}{n_1}+\pi\frac{n_2}{n_1}\right)\right)\left(1+\cos\left(\frac{2\pi kN}{n_2}\right)\right)\left(1+\cos\left(\frac{2\pi kN}{n_5}\right)\right), \end{aligned} \tag{3.17}$$

and at detector C the intensity is

$$\begin{aligned} I_C &= \frac{1}{8}\sum_{k=1}^{n_7}\left(1+\cos\left(\frac{2\pi(kN+n_2/2)}{n_1}\right)\right)\left(1-\cos\left(\frac{2\pi(kN+n_2/2)}{n_2}\right)\right)\left(1-\cos\left(\frac{2\pi kN}{n_5}\right)\right) \\ &\approx \frac{1}{8}\sum_{k=1}^{n_7}\left(1+\cos\left(\frac{2\pi kN}{n_1}+\pi\frac{n_2}{n_1}\right)\right)\left(1+\cos\left(\frac{2\pi kN}{n_2}\right)\right)\left(1-\cos\left(\frac{2\pi kN}{n_5}\right)\right), \end{aligned} \tag{3.18}$$

if we assume that $2 \cdot \lfloor n_2/2 \rfloor \approx n_2$. This may cause problems for small, odd integers n_2. However, one can argue that testing small integers for being factors of N is simple and not primarily of interest here. In addition, we need that $n_2/n_1 \neq 2m+1$ for $m \in \mathbb{N}$ such that the first factor in Eqs. (3.17) and (3.18) does not vanish if n_1 is a factor of N. Nevertheless, the shift of the argument of the cosine by $\pi n_2/n_1$ can lead to a reduction in the intensity. For example for $n_2/n_1 \approx 3/2$ and n_1 a factor of N, the first factor would be a 1 instead of a 2.

In order to check whether n_6 is a factor of N, we have to wait twice. First we have to wait for $n_1/2$ steps for the increment of χ_3 to start, and then we have to wait for another $n_3/2$ steps until we can start incrementing the phase χ_6. So for the intensity at detector E we obtain

$$\begin{aligned} I_E &= \frac{1}{8}\sum_{k=1}^{n_7}\left(1-\cos\left(\frac{2\pi(kN+n_1/2+n_3/2)}{n_1}\right)\right)\left(1-\cos\left(\frac{2\pi(kN+n_3/2)}{n_3}\right)\right)\left(1+\cos\left(\frac{2\pi kN}{n_6}\right)\right) \\ &\approx \frac{1}{8}\sum_{k=1}^{n_7}\left(1-\cos\left(\frac{2\pi kN}{n_1}+\pi\left(1+\frac{n_3}{n_1}\right)\right)\right)\left(1-\cos\left(\frac{2\pi kN}{n_3}+\pi\right)\right)\left(1+\cos\left(\frac{2\pi kN}{n_6}\right)\right) \\ &= \frac{1}{8}\sum_{k=1}^{n_7}\left(1+\cos\left(\frac{2\pi kN}{n_1}+\pi\frac{n_3}{n_1}\right)\right)\left(1+\cos\left(\frac{2\pi kN}{n_3}\right)\right)\left(1+\cos\left(\frac{2\pi kN}{n_6}\right)\right), \end{aligned} \tag{3.19}$$

and for detector F we have

$$\begin{aligned} I_F &= \frac{1}{8}\sum_{k=1}^{n_7}\left(1-\cos\left(\frac{2\pi(kN+n_1/2+n_3/2)}{n_1}\right)\right)\left(1-\cos\left(\frac{2\pi(kN+n_3/2)}{n_3}\right)\right)\left(1-\cos\left(\frac{2\pi kN}{n_6}\right)\right) \\ &\approx \frac{1}{8}\sum_{k=1}^{n_7}\left(1+\cos\left(\frac{2\pi kN}{n_1}+\pi\frac{n_3}{n_1}\right)\right)\left(1+\cos\left(\frac{2\pi kN}{n_3}\right)\right)\left(1-\cos\left(\frac{2\pi kN}{n_6}\right)\right), \end{aligned} \tag{3.20}$$

where we again used the assumptions that $2 \cdot \lfloor n_1/2 \rfloor \approx n_1$ and $2 \cdot \lfloor n_3/2 \rfloor \approx n_3$. As in the case of detectors C and D, we have the additional constraint that $n_3/n_1 \neq 2m+1$ for $m \in \mathbb{N}$ such that the first factor does not vanish if n_1 is a factor of N. If n_2 and n_3 are prime, which is a reasonable assumption, n_2/n_1 and n_3/n_1 cannot be integers, and thus also not odd integers. Nonetheless, severe reductions in the intensities are still possible.

In addition to all these assumptions and approximations, there is still the approximation mentioned before in Eq. (3.8) which we need to generate a table with (approximate) expectations ignoring the dependencies on N and the n_i, $i = 1, 2, \ldots, 7$ such that we have an N and n_i-independent look-up table. An excerpt is given in Table 3.5. However, in this excerpt we can already see that the intensity distributions are not unique which is a problem if we want to use them for the identification of factors of N. For seven Mach-Zehnder interferometers, there is only one intensity distribution which occurs twice, but for extensions to more interferometers, and thus testing for more possible factors at a time, duplicates may occur even more often.

At this point, we have to come back to the small increments proposed by Summhammer and mentioned in the beginning as here we need to be able to start the increments of χ_3, χ_5, χ_6 and χ_7 when χ_1, χ_2 and χ_4 are not multiples of $2\pi N/n_i$, $i = 1, 2, 4$. So in the simulation, the phases are computed from $l = N$ up to $l = N \cdot n_7 + \lfloor n_1/2 \rfloor + \lfloor n_3/2 \rfloor$

according to

$$\chi_1(l) = \frac{2\pi l}{n_1} \qquad \chi_2(l) = \frac{2\pi l}{n_1} \qquad \chi_4(l) = \frac{2\pi l}{n_4}, \tag{3.21}$$

$$\chi_3(l) = \frac{2\pi(l - \lfloor \frac{n_1}{2} \rfloor)}{n_3} \qquad \chi_7(l) = \frac{2\pi(l - \lfloor \frac{n_1}{2} \rfloor)}{n_7} \qquad l \geq N + \lfloor \tfrac{n_1}{2} \rfloor, \tag{3.22}$$

$$\chi_5(l) = \frac{2\pi(l - \lfloor \frac{n_2}{2} \rfloor)}{n_5} \qquad l \geq N + \lfloor \tfrac{n_2}{2} \rfloor, \tag{3.23}$$

$$\chi_6(l) = \frac{2\pi(l - \lfloor \frac{n_1}{2} \rfloor - \lfloor \frac{n_3}{2} \rfloor)}{n_6} \qquad l \geq N + \lfloor \tfrac{n_1}{2} \rfloor + \lfloor \tfrac{n_3}{2} \rfloor. \tag{3.24}$$

So the phases are incremented by $2\pi/n_i$, $i = 1, 2, \ldots, 7$, but the messengers are only counted if they arrive

- at detectors A or B if $l \bmod N = 0$ and $l \leq N \cdot n_7$
- at detectors C or D if $l \bmod N = \lfloor \frac{n_2}{2} \rfloor$ and $l \leq N \cdot n_7 + \lfloor \frac{n_2}{2} \rfloor$
- at detectors E or F if $l \bmod N = \lfloor \frac{n_1}{2} \rfloor + \lfloor \frac{n_3}{2} \rfloor$ and $l \leq N \cdot n_7 + \lfloor \frac{n_1}{2} \rfloor + \lfloor \frac{n_3}{2} \rfloor$
- at detectors G or H if $l \bmod N = \lfloor \frac{n_1}{2} \rfloor$ and $l \leq N \cdot n_7 + \lfloor \frac{n_1}{2} \rfloor$.

In this way, at each detector n_7 settings are regarded. Thus, for the normalization we can again divide the counters, which count the messengers arriving at the detectors for correct settings, by Ln_7. For this case we used $L = 100\,000$.

Since the N and n_i-independent table is obtained by making more approximations than in the previous case, we again give for each simulation of a set of n_i, $i = 1, \ldots, 7$, and N also the numerical evaluation of the exact intensities. The results are given in Table 3.6. The intensities resulting from the simulation and the numerical evaluation coincide with each other. However, we see that the intensity distributions cannot be used to identify factors of N. For example for $N = 261$ and $N = 217$, only n_1 is a factor but the intensity distributions differ widely and none coincides with the corresponding distribution given in Table 3.5. So the actual intensity distributions depend heavily on the numbers n_i, $i = 1, 2, \ldots, 7$, and N.

Compared to the complex version discussed in this section, the simple extension from the previous section has more advantages. So there are only n_7 consecutive, larger increments of all phase shifters necessary, whereas in the more complex version $N \cdot n_7$ consecutive, smaller increments are needed. So if we assume in a serious application $n_7 \leq \sqrt{N}$, we have a complexity of $\sqrt{N}$ for finding one factor using the simple version. If we want to find all factors, we have to apply the procedure more often, but not more than $\lfloor \log_2(N) + 1 \rfloor$ times in the worst case as there cannot be more factors. Thus we are still at a complexity of $\sqrt{N} \log_2(N)$ which is less than $N^{3/2}$ for the proposal by Summhammer [22] for the more complex version. The results of the exact evaluations deviate much more from the N and n_i-independent table for the more complex version than for the simple case due to more approximations, making the identification of the factors difficult to even nearly impossible in some cases. Moreover, the table, which is derived for this more complicated version, is not even unique in the sense that in two cases not even one factor can be determined with certainty. Therefore, we think the simple version is more useful.

Table 3.5: Excerpt of the expected intensities when eliminating the dependence on the n_i, $i = 1, 2, \ldots, 7$, to have general relations. As before, "F" denotes factors of N, and "–" denotes nonfactors. We see that the intensity distributions for n_1 being a factor and for n_2 and n_3 being factors are identical (highlighted in yellow).

n_1	n_2	n_3	n_4	n_5	n_6	n_7	I_A	I_B	I_C	I_D	I_E	I_F	I_G	I_H
-	-	-	-	-	-	-	0.125	0.125	0.125	0.125	0.125	0.125	0.125	0.125
F	-	-	-	-	-	-	0.25	0.25	0.25	0.25	0.25	0.25	0.25	0.25
-	F	-	-	-	-	-	0.25	0.25	0.25	0.25	0.125	0.125	0.125	0.125
F	F	-	-	-	-	-	0.5	0.5	0.5	0.5	0.25	0.25	0.25	0.25
-	-	F	-	-	-	-	0.125	0.125	0.125	0.125	0.25	0.25	0.25	0.25
F	-	F	-	-	-	-	0.25	0.25	0.25	0.25	0.5	0.5	0.5	0.5
-	F	F	-	-	-	-	0.25	0.25	0.25	0.25	0.25	0.25	0.25	0.25
F	F	F	-	-	-	-	0.5	0.5	0.5	0.5	0.5	0.5	0.5	0.5
-	-	-	F	-	-	-	0.25	0	0.125	0.125	0.125	0.125	0.125	0.125
F	-	-	F	-	-	-	0.5	0	0.25	0.25	0.25	0.25	0.25	0.25
-	F	-	F	-	-	-	0.5	0	0.25	0.25	0.125	0.125	0.125	0.125
F	F	-	F	-	-	-	1	0	0.5	0.5	0.25	0.25	0.25	0.25
-	-	F	F	-	-	-	0.25	0	0.125	0.125	0.25	0.25	0.25	0.25
F	-	F	F	-	-	-	0.5	0	0.25	0.25	0.5	0.5	0.5	0.5
-	F	F	F	-	-	-	0.5	0	0.25	0.25	0.25	0.25	0.25	0.25
F	F	F	F	-	-	-	1	0	0.5	0.5	0.5	0.5	0.5	0.5

Table 3.6: Results for the intensities at the detectors A through H for the discrete-event simulation (upper rows) and for the numerical evaluation of the sums (lower rows) dependent on the possible factors n_i, $i = 1, 2, \ldots, 7$, of N.

N	n_1	n_2	n_3	n_4	n_5	n_6	n_7	I_A	I_B	I_C	I_D	I_E	I_F	I_G	I_H
529	3	5	7	11	13	17	19	0.083	0.138	0.097	0.170	0.142	0.097	0.117	0.120
								0.082	0.139	0.097	0.171	0.142	0.097	0.118	0.119
261	3	7	11	13	17	19	23	0.202	0.272	0.263	0.219	0.001	0.001	0.200	0.173
								0.203	0.273	0.264	0.219	0	0	0.200	0.172
217	7	11	13	17	19	23	29	0.247	0.247	0.096	0.096	0.142	0.162	0.233	0.238
								0.247	0.247	0.097	0.096	0.141	0.162	0.234	0.238
345	3	5	7	11	13	17	19	0.492	0.503	0.116	0.110	0.223	0.145	0.186	0.173
								0.495	0.505	0.116	0.110	0.224	0.146	0.186	0.173
693	3	5	7	11	13	17	19	0.472	0.001	0.067	0.054	0.339	0.371	0.372	0.374
								0.474	0	0.066	0.053	0.340	0.373	0.375	0.375
115	3	5	7	11	13	17	19	0.235	0.250	0.229	0.246	0.098	0.141	0.127	0.110
								0.236	0.251	0.229	0.247	0.098	0.141	0.128	0.109
325	3	5	7	11	13	17	19	0.235	0.250	0.001	0.474	0.134	0.105	0.095	0.142
								0.236	0.251	0	0.476	0.134	0.105	0.095	0.142
143	7	11	13	17	19	23	29	0.233	0.250	0.278	0.221	0.246	0.249	0.249	0.239
								0.234	0.251	0.279	0.221	0.247	0.250	0.250	0.239
169	7	11	13	17	19	23	29	0.100	0.141	0.123	0.118	0.256	0.251	0.276	0.238
								0.100	0.141	0.123	0.118	0.257	0.251	0.277	0.239
299	7	11	13	17	19	23	29	0.109	0.137	0.146	0.101	0.473	0.001	0.260	0.228
								0.109	0.137	0.146	0.101	0.476	0	0.261	0.228
377	7	11	13	17	19	23	29	0.120	0.127	0.085	0.159	0.238	0.243	0.001	0.501
								0.119	0.126	0.085	0.159	0.239	0.244	0	0.504
323	7	11	13	17	19	23	29	0.240	0.001	0.001	0.240	0.088	0.069	0.070	0.187
								0.241	0	0	0.241	0.087	0.068	0.070	0.187

4 Quantum Random Walk

In this chapter, we discuss the quantum random walk after a short introduction of the classical counterpart, the random walk. We also examine discrete-event simulations of the random walk and the quantum random walk. Furthermore, we apply these simulations to the experiments of quantum random walks presented in [23] and [24] which have been performed in the laboratory.

In the experiments and simulations that we consider, the walker moves to the left or to the right with probability one half in the classical case, and a balanced superposition is created in the quantum case. This property is also called *fair coin toss* as left and right are equally likely just like head or tails are equally probable in a coin toss with a fair coin.

We especially examine an experiment that is used to show a violation of the Leggett-Garg inequality, which we also discuss in that given context. For this experiment, our aim is to show that we can use the discrete-event simulation to produce data that either violates or does not violate the Leggett-Garg inequality depending on the evaluation method. If we are able of doing so, this means that not the quantum random walk itself violates the Leggett-Garg inequality but the evaluation method plays an important part.

We will see that we are capable of reproducing the results of the quantum random walk experiments with the discrete-event simulation, and also to perform non-invasive measurements which leads to the Leggett-Garg inequality not being violated.

4.1 Classical Random Walk

Before we investigate the quantum walk, we summarize the most important facts about the classical random walk (in one dimension). Discrete and continuous random walks in more than one dimension play an important role in many fields in natural sciences such as in physics and chemistry where the connection comes through the diffusion equation [25], but also in biology [25] [26] [27] and computer science [28] [29] (here especially in graph theory) the random walk is often applicable.

Here, we will only discuss the discrete random walk which can be illustrated by a particle starting at position $x = 0$, which can in each time step move one step to the left or to the right with probability one half each. So the particle can only move in integer steps such that allowed positions are $x = k$, where $k \in \mathbb{Z}$. After l steps, the probability to find the particle at position $x = k$ is given by

$$P(k,l) = \begin{cases} 2^{-l} \begin{pmatrix} l \\ \frac{k+l}{2} \end{pmatrix} & \text{if } l+k \text{ is even} \\ 0 & \text{otherwise} \end{cases}. \tag{4.1}$$

Table 4.1 contains the probabilities for $l = 1, \ldots, 5$. Since the probability distribution is symmetric in k for all l, the expectation value of the position, $\langle x \rangle$, is equal to zero for all

numbers of time steps l. For the random walk, the variance of the position, $\langle x^2\rangle - \langle x\rangle^2$, scales linearly with l (in fact for our choice of integer steps, with a slope of one) [25]:

$$\langle x^2\rangle - \langle x\rangle^2 = \langle x^2\rangle = l. \tag{4.2}$$

For the simulation of a random walk with l time steps, we need an array `D` of length $2l+1$ for the possible positions $x \in \{-l,\ -l+1, \ldots,\ l-1,\ l\}$ as after l time steps a particle can maximally end up at the position $x = \pm l$. Apart from that we need a position counter `pos_count` initialized to zero to keep track of the particle's position. For each time step a (pseudo) random number $r \in \{-1, 1\}$ is added to the position counter. After l time steps, the detector at position `pos_count` detects a particle, i.e., the entry `pos_count` $+ l$ of the detector array `D` is incremented by one. When this is done for a total number N of particles, `D`$[i]/N$ for $i \in \{0,\ 1,\ 2, \ldots,\ 2l\}$ is written to a file for plotting.

Table 4.1: Probability distributions of the random walk after $l = 1, \ldots, 5$ time steps. The distributions are symmetric with a peak around $k = 0$ and decreasing probabilities at the edges. Also clearly visible are the facts that only every second position can be occupied and the spread of possibly occupied positions increases with l.

Time steps	Position k										
l	-5	-4	-3	-2	-1	0	1	2	3	4	5
1	0	0	0	0	$1/2$	0	$1/2$	0	0	0	0
2	0	0	0	$1/4$	0	$1/2$	0	$1/4$	0	0	0
3	0	0	$1/8$	0	$3/8$	0	$3/8$	0	$1/8$	0	0
4	0	$1/16$	0	$1/4$	0	$3/8$	0	$1/4$	0	$1/16$	0
5	$1/32$	0	$5/32$	0	$5/16$	0	$5/16$	0	$5/32$	0	$1/32$

The normalized number of detector counts N_x/N as a function of the detector number x for l between 2 and 7 are shown in Fig. 4.1 and for $l = 19, 20$ in Fig. 4.2. The binomial shape of the distributions is clearly visible. Due to the symmetry, the mean is zero for all numbers of steps. Since the distribution spreads with an increasing number of steps, the variance grows with the number of steps l. In fact, the variance grows linearly with a slope of one as illustrated in Fig. 4.3 and theoretically expected, see Eq. (4.2).

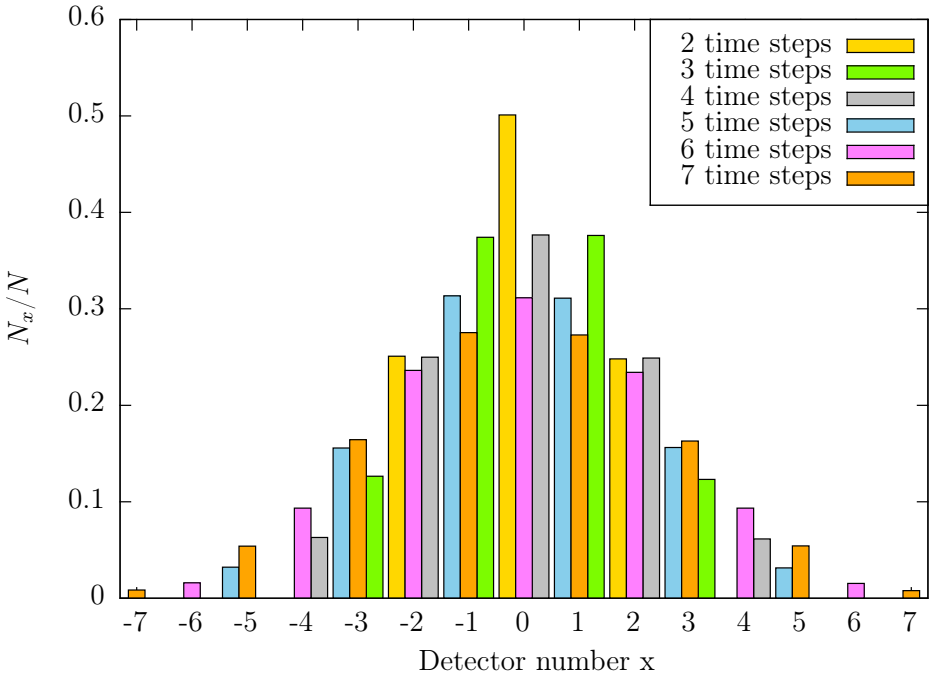

Figure 4.1: Results of the normalized number of detector counts N_x/N as a function of the detector number x of the simulation of the random walk for 2 up to 7 time steps. The distributions are always symmetric and for an even (odd) number of steps only the detectors at even (odd) positions detect particles.

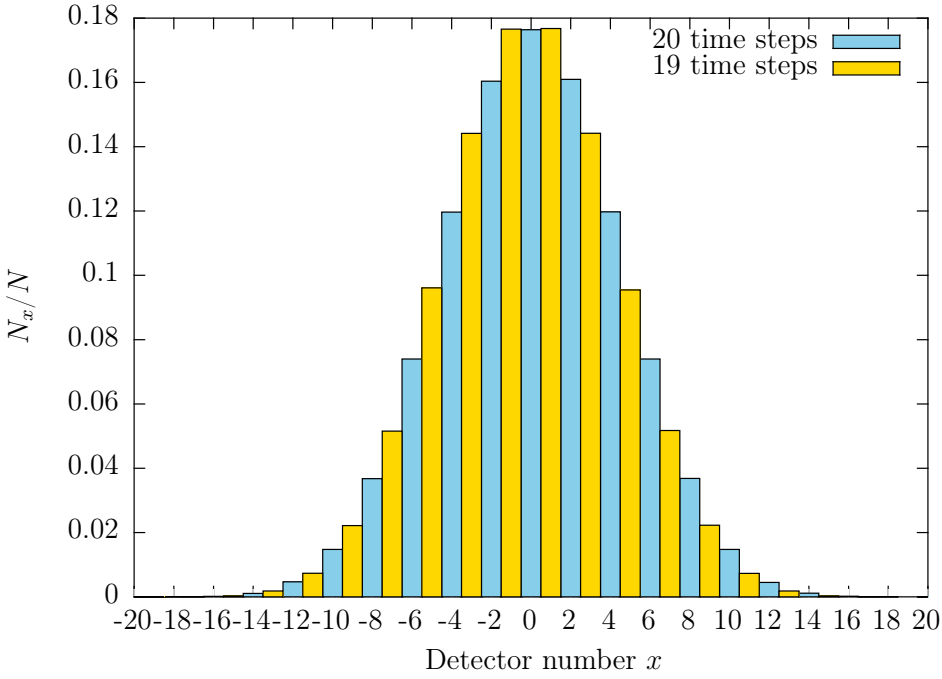

Figure 4.2: Normalized number of detector counts N_x/N as a function of the detector number x for the simulation of the classical random walk after 19 and 20 time steps.

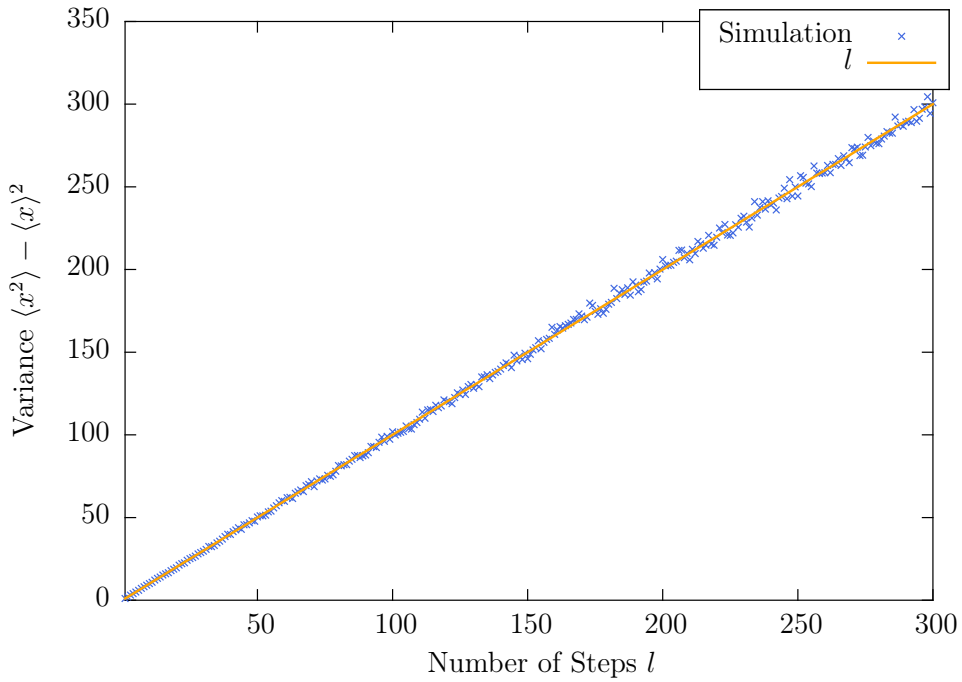

Figure 4.3: Variance of the random walk depending on the number of time steps l. The blue crosses originate from the simulation and agree nicely with the orange straight line of slope one which is the expectation from the theory.

In summary, for the classical random walk we have that the probability distribution of the position is a binomial distribution, i.e., it is symmetric around zero, and therefore its mean is also zero. The distribution widens with an increasing number of steps such that the variance grows linearly. Furthermore, the probability to find a particle at an odd (even) position after an even (odd) number of steps is zero. In contrast, we will now investigate the properties of the quantum walk in the following section.

4.2 Quantum Walk

After the discussion of the classical random walk, we now have a look at the quantum version of the random walk. The quantum random walk or quantum walk was first introduced in 1993 [30]. Then it was named *quantum random walk* by analogy to the (classical) random walk. But since the quantum random walk is actually not random but deterministic (it can be reversed as shown in Ref. [31]), it was later usually called *quantum walk*.

As the classical random walk is used for many classical algorithms, researchers also examine the quantum walk in order to find applications to quantum algorithms [32]. There are various kinds of proposals and implementations of the quantum walk using optical lattices [24] [33] [34], ion traps [35] [36] [31], microwave cavities [37], or optical networks [23] [38] [39]. So in recent years, the quantum walk has attracted great interest in science.

The idea of the quantum walk is similar to that of the classical random walk. In each step, the particle's position x can either increase or decrease by a discrete step of length one, depending on another degree of freedom of dimension two of the particle such as its

spin. The particle is shifted to the right if its spin is up ($|\uparrow\rangle$) and to the left if its spin is down ($|\downarrow\rangle$), for example. However, the particle's spin is not necessarily fixed to spin up or spin down. It can also be prepared in a superposition of both, e.g., spin up in the σ_x-basis at position $x = 0$: $(|\uparrow\rangle + |\downarrow\rangle) \otimes |0\rangle/\sqrt{2}$. After the shift, the particle is in a superposition: $(|\uparrow, 1\rangle + |\downarrow, -1\rangle)/\sqrt{2}$. Next, at each new position of the particle the transformation creating the superposition of spin up and spin down is applied, followed by the shifting. Of interest is that in the quantum case the particle produces an interference pattern at the detector plane. Unlike in the classical case, the detected pattern is not necessarily symmetric. Also the variance grows faster. A detailed introduction to quantum walks is given in Ref. [40].

Mathematically, the quantum walk is usually performed by making use of the Hadamard operation

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \tag{4.3}$$

or a similar transformation to create the superposition in the two-dimensional Hilbert space $\mathcal{H}_\mathcal{S} = \text{span}\{|\uparrow\rangle,\ |\downarrow\rangle\} \cong \mathbb{C}^2$ of the degree of freedom (the spin notation is used to avoid confusion with the position space). For the position space any Hilbert space isomorphic to $\mathcal{H}_\mathcal{P} = \text{span}\{|k\rangle \,|\, k \in \mathbb{Z}\}$ can be used. The particle shift can be described by the following operator acting on $\mathcal{H}_\mathcal{S} \otimes \mathcal{H}_\mathcal{P}$

$$S = |\uparrow\rangle\langle\uparrow| \otimes \sum_k |k+1\rangle\langle k| + |\downarrow\rangle\langle\downarrow| \otimes \sum_k |k-1\rangle\langle k|. \tag{4.4}$$

After l steps, the particle is in the state $|\psi_l\rangle = (S(H \otimes I_P))^l |\psi_0\rangle$ where I_P is the identity operator acting on $\mathcal{H}_\mathcal{P}$, H is the transformation creating the superposition, and $|\psi_0\rangle$ is the initial state, e.g. $|\psi_0\rangle = |\uparrow\rangle \otimes |0\rangle$.

In the following, we implement the quantum walk by means of the discrete-event simulation method described in chapter 2.

4.2.1 Discrete-Event Simulation of a Quantum Walk

In this section, we describe an implementation of the quantum walk by means of a discrete-event simulation. For the simulation of the quantum walk, we use a scheme which is introduced in Ref. [23] by Jeong, Paternostro, and Kim to perform a quantum walk using a classical light field. They only use optical elements like 50:50 beam splitters, phase shifters, and photodetectors which are arranged as depicted in Fig. 4.4. The beam splitters are used to create the superposition of the two input modes. The matrix representation of a beam splitter is given by

$$M_{\text{BS}} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}. \tag{4.5}$$

As the beam splitter produces relative phases that differ from those of the Hadamard transformation (see Eq. (4.3)), two phase shifters having the Jones matrix representation

$$M_{\varphi_1} = \begin{pmatrix} e^{i\varphi_1} & 0 \\ 0 & 1 \end{pmatrix} \text{ and } M_{\varphi_2} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\varphi_2} \end{pmatrix}, \tag{4.6}$$

where φ_1 and φ_2 denote the phases of the shifters, are inserted around the beam splitters to compensate for these phase differences. This scheme is well-suited for a discrete-event simulation of the quantum walk because it requires only a few simple optical elements. The most sophisticated element is the 50:50 beam splitter which is implemented as described in section 2.5 by means of a stochastic learning machine. We first consider the analytical outcomes to later compare the simulation results with them.

In order to compute the analytical outcomes for an arbitrary number of levels of the scheme depicted in Fig. 4.4, we have to find a canonical description of each step of the calculation to implement it iteratively in, e.g., MATHEMATICA in finite vector spaces. For this purpose we introduce vectors $|j\rangle$ labeled as shown in Fig. 4.5. As this labeling is a bit different from the usual labeling (but it simplifies the program in MATHEMATICA), the difference is illustrated in Fig. 4.6 for clarity. This kind of labeling leads to the beam splitter operation B_{jk} acting on the vectors $|j\rangle$ and $|k\rangle$ being written as

$$B_{jk} = \frac{1}{\sqrt{2}} \left(i|j\rangle\langle j| + |k\rangle\langle j| + |j\rangle\langle k| + i|k\rangle\langle k| \right), \tag{4.7}$$

and the operation T_{jk} consisting of the combination of two phase shifters and the beam splitter (marked by the gray dashed boxes in Fig. 4.4) is given by

$$T_{jk} = \frac{1}{\sqrt{2}} \left(ie^{i(\varphi_1+\varphi_2)}|j\rangle\langle j| + e^{i\varphi_1}|k\rangle\langle j| + e^{i\varphi_2}|j\rangle\langle k| + i|k\rangle\langle k| \right). \tag{4.8}$$

For the 2-level quantum walk, for example, one has to compute

$$(T_{12} + T_{34})\, B_{23}|2\rangle = (T_{12} + T_{34}) \frac{1}{\sqrt{2}} \left(i|2\rangle + |3\rangle \right) = \frac{1}{2} \left(ie^{i\varphi_2}|1\rangle - |2\rangle + ie^{i(\varphi_1+\varphi_2)}|3\rangle + e^{i\varphi_1}|4\rangle \right), \tag{4.9}$$

and then add the absolute values squared of the coefficients of the vectors $|4\rangle$, $|2\rangle$ and $|3\rangle$, $|1\rangle$, respectively, to obtain probabilities $P_2(-2)$, $P_2(0)$, and $P_2(2)$ of detection events at detectors D_{-2}, D_0, and D_2, respectively. Here, the detectors are labeled by even integers for an even number of levels, and for an odd number of levels the detectors are labeled accordingly by odd numbers. This results in $P_2(-2) = |ie^{i\varphi_1}|^2/4 = 1/4$ for detector D_{-2}, $P_2(0) = |-1|^2/4 + |ie^{i(\varphi_1+\varphi_2)}|^2/4 = 1/2$ for detector D_0, and $P_2(2) = |e^{i\varphi_2}|^2/4 = 1/4$ for detector D_2.

In general, the probability distributions for up to l levels are computed iteratively as follows. The states $|\xi_j\rangle$ after the j-th level ($j = 1, \ldots, l$) are

$$\begin{aligned}
|\xi_1\rangle &= B_{l,l+1}|l\rangle \\
|\xi_2\rangle &= (T_{l-1,l} + T_{l+1,l+2})|\xi_1\rangle \\
&\vdots \\
|\xi_j\rangle &= (T_{l-j+1,l-j+2} + T_{l-j+3,l-j+4} + \cdots + T_{l+j-1,l+j})|\xi_{j-1}\rangle \\
&\vdots \\
|\xi_l\rangle &= (T_{12} + T_{34} + \cdots + T_{2l-1,2l})|\xi_{l-1}\rangle.
\end{aligned} \tag{4.10}$$

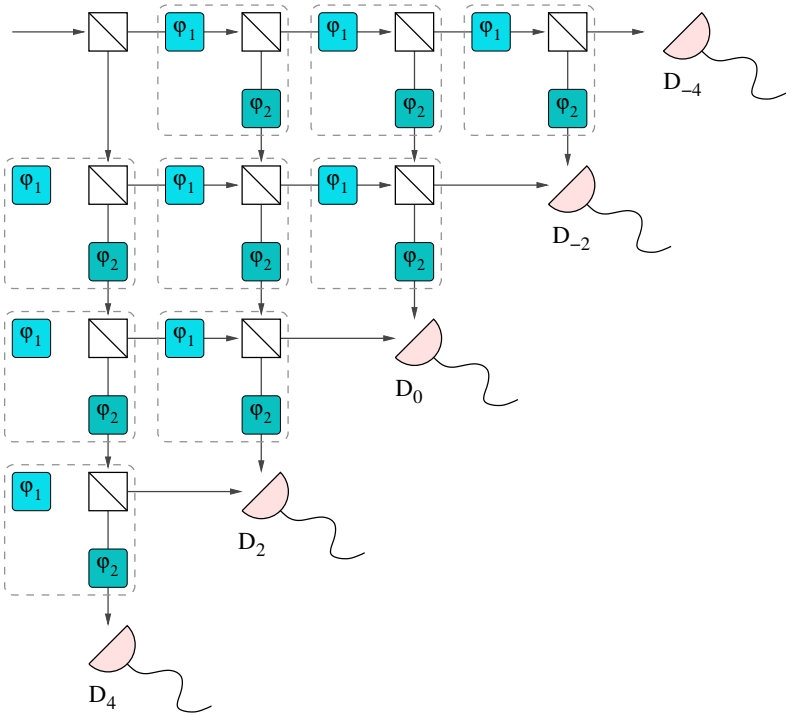

Figure 4.4: Setup for the quantum walk as proposed in Ref. [23] for the example of the 4-level quantum walk. The cyan boxes represent phase shifters with an angle φ_1 or φ_2, respectively. White boxes with a diagonal line represent 50:50 beam splitters and pink half circles with a tail denote detectors, which are labeled in the same way as in Ref. [23].

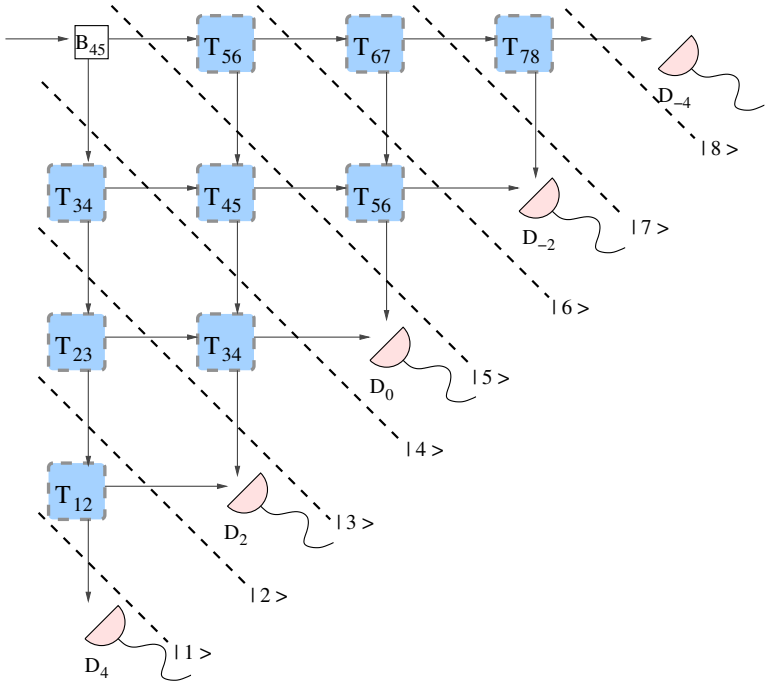

Figure 4.5: Visualization of the labeling of the vectors for the analytical calculation. Blue dashed boxes represent phase shifters and one beam splitter as enclosed by a gray dashed line in Fig. 4.4. Black dashed lines illustrate which positions are labeled by which state $|j\rangle$, $j \in \{1, \ldots, 2l\}$ where l is the number of levels. The direction of the moves of the photons is represented by the asymmetry of the definition of the T_{jk} (see Eq. (4.8)).

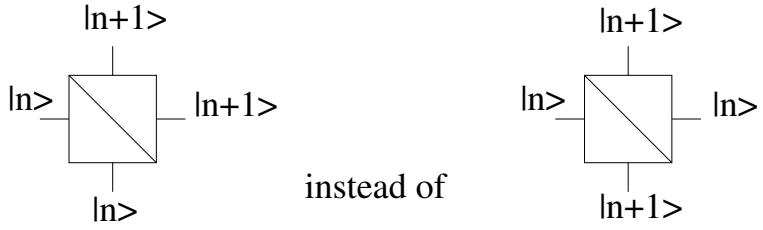

Figure 4.6: Sketch which stresses the difference between the usual basis (right) and the one used for the computation with MATHEMATICA (left). The squares with the diagonal line represent beam splitters, and $|n\rangle$ and $|n+1\rangle$ denote basis vectors with $n \in \{1, 2, \ldots, 2l-1\}$ where l is the number of levels.

The probability $P_j(x)$ for a photon to be detected at detector x after going through j levels is then obtained by summing up the squared absolute values of adjacent vectors, as visualized in Fig. 4.5 for an even number of levels, with $k \in \{-j/2, -j/2+1, \ldots, j/2-1, j/2\}$:

$$P_j(x) = \begin{cases} |\langle l-2k|\xi_j\rangle|^2 + |\langle l-2k+1|\xi_j\rangle|^2 & \text{if } x = 2k \\ 0 & \text{otherwise} \end{cases}. \tag{4.11}$$

For j even, $2k$ is also even, and for j odd, $2k$ is also odd, so photons can only be detected in even or odd detectors depending on the number of levels.

In the MATHEMATICA program that implements this procedure the standard basis $\{e_j \,|\, j = 1, ..., 2l\}$ is used for the abstract vectors $\{|j\rangle \,|\, j = 1, ..., 2l\}$ where l is the number of levels. In Table 4.2, the analytical expressions for up to 5 levels are shown. The dependence on φ_2 is visualized in Fig. 4.7 taking 7 levels as an example. For a fixed $\varphi_2 = -\pi/2$, the distributions for up to ten levels are depicted in Fig. 4.8.

Table 4.2: Analytical results for the probability distributions of the quantum walk for levels 1 to 5. The distributions only depend on φ_2 and are independent of φ_1. The distributions for more than 2 levels can be either symmetric or asymmetric w.r.t. $x = 0$ depending on φ_2. For levels 1 and 2, the distributions are symmetric and coincide with the ones of the classical random walk.

Level	Detector number										
	-5	-4	-3	-2	-1	0	1	2	3	4	5
1	0	0	0	0	$\frac{1}{2}$	0	$\frac{1}{2}$	0	0	0	0
2	0	0	0	$\frac{1}{4}$	0	$\frac{1}{2}$	0	$\frac{1}{4}$	0	0	0
3	0	0	$\frac{1}{8}$	0	$\frac{3-2\cos\varphi_2}{8}$	0	$\frac{3+2\cos\varphi_2}{8}$	0	$\frac{1}{8}$	0	0
4	0	$\frac{1}{16}$	0	$\frac{3-2\cos\varphi_2}{8}$	0	$\frac{1}{8}$	0	$\frac{3+2\cos\varphi_2}{8}$	0	$\frac{1}{16}$	0
5	$\frac{1}{32}$	0	$\frac{11-6\cos\varphi_2}{32}$	0	$\frac{1}{8}$	0	$\frac{1}{8}$	0	$\frac{11+6\cos\varphi_2}{32}$	0	$\frac{1}{32}$

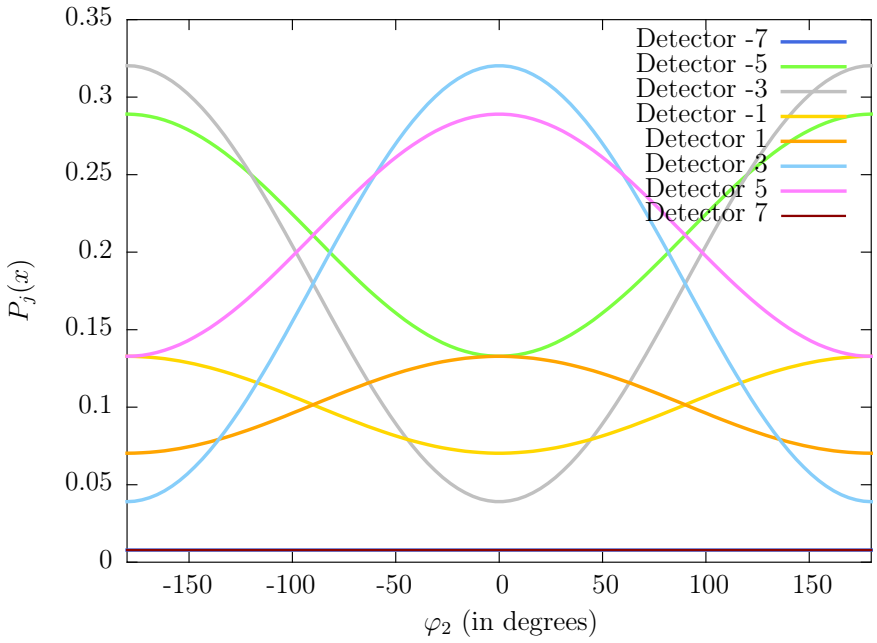

Figure 4.7: Dependence of the probability distribution $P_j(x)$ on the phase shift φ_2 for each detector x in the 7-level quantum walk. The curves for detectors $x = -7$ and $x = 7$ are equal and constant. For $\varphi_2 = \pm 90°$, the detectors x and $-x$ for $x = 1, 3, 5, 7$ count the same amount of particles and therefore the distribution is symmetric for this setting.

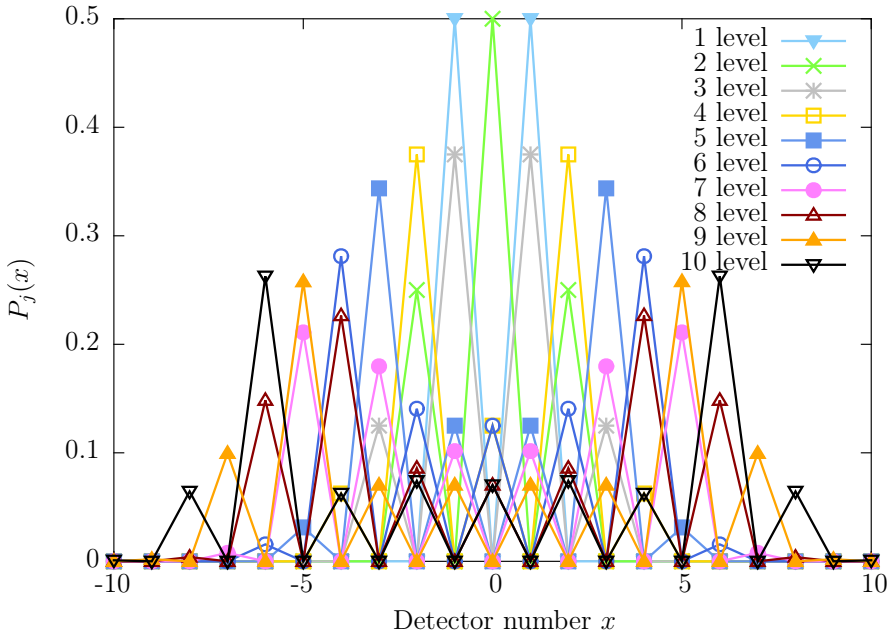

Figure 4.8: Visualization of the analytical results of the quantum walk for $\varphi_2 = -\pi/2$ for up to ten levels. The lines are guides to the eye only. The deviation from the classical random walk is clear as with an increasing number of levels, the maxima of the distributions move (in this case symmetrically) away from the center to the margins.

The analytical results given in Table 4.2 show that the distributions do not depend on φ_1, and that for more than 2 levels the dependence on φ_2 is given by scaled and

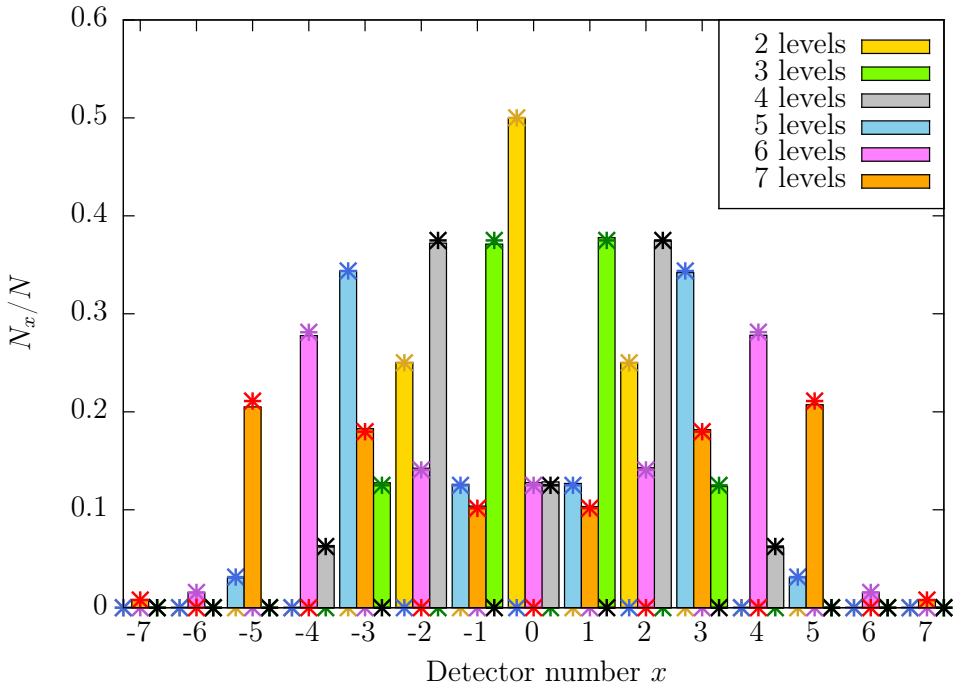

Figure 4.9: Results for the normalized number of detector counts N_x/N as a function of the detector number x, obtained by a discrete-event simulation of the quantum walk for $N = 100\,000$ repetitions, $\varphi_1 = \pi/2$ and $\varphi_2 = -\pi/2$ and for different numbers of levels. Compared to the classical random walk (see Fig. 4.1), for more than 3 levels the distributions differ because interference becomes important. The distributions match with the analytical expectation visualized by stars in a darker shade of the color corresponding to the number of levels.

shifted cosines. The deviations from the classical distribution are caused by interference effects. These deviations can also be seen in Fig. 4.7 where the dependence on φ_2 is clearly visible: The distribution is not symmetric w.r.t. $x = 0$ like in the classical case except for $\varphi_2 = \pm 90°$. For $\varphi_2 = 0°$ and $\varphi_2 = \pm 180°$, the asymmetry is strongest. In Fig. 4.8, one can see how the maxima of the distribution move outwards for a larger number of levels. Moreover, it is clearly visible that detectors with an odd (even) number only register particles if the number of levels is also odd (even).

In what follows, we discuss the results of the discrete-event simulation of the quantum walk. We use the setup shown in Fig. 4.4 and presented in Ref. [23]. In the discrete-event simulation, at any time there is only one photon in the setup. Only after the arrival of a photon at the detector another photon is sent. The simulation supports arbitrarily many levels. The number of photons sent through the setup per run has to be increased starting from a given number of levels because the number of beam splitters grows, and for the beam splitters to work properly, a certain number of photons must have passed through them. For each run, we send $N = 100\,000$ photons through the setup. This is sufficient to go up to 7 levels and collect good statistics. The results of the simulations for 2 up to 7 levels and for the angles $\varphi_1 = \pi/2$ and $\varphi_2 = -\pi/2$, which are the angles chosen in the experiment [23], are shown in Fig. 4.9. The outcomes agree with the analytical results, so the discrete-event simulation of the quantum walk indeed produces the quantum result.

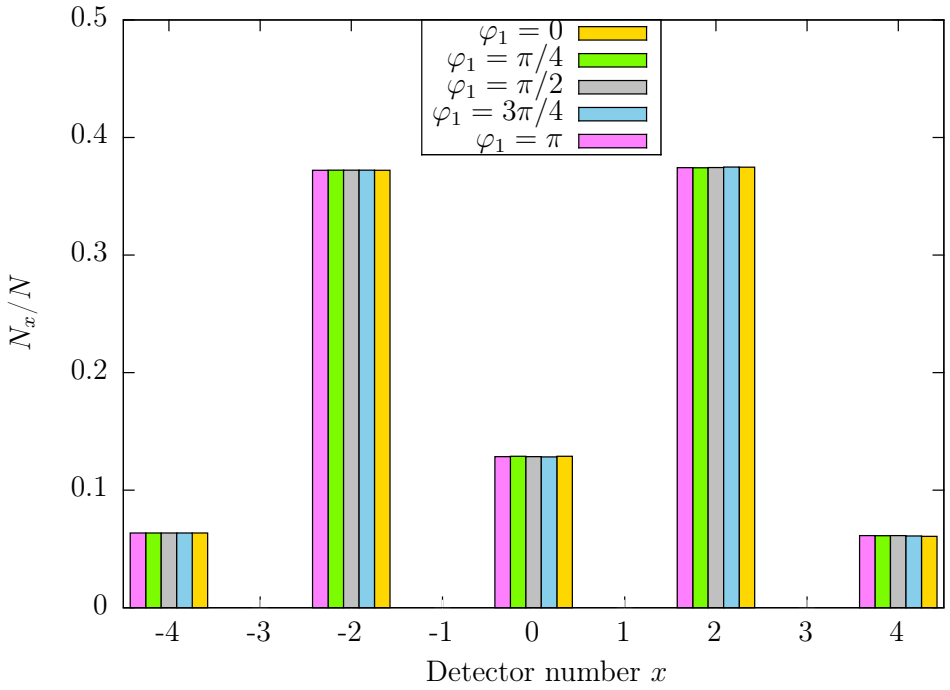

Figure 4.10: Dependence of the simulated distribution N_x/N on the detector number x for the 4-level quantum walk for various angles φ_1 and $\varphi_2 = -\pi/2$. The number of repetitions is $N = 100\,000$.

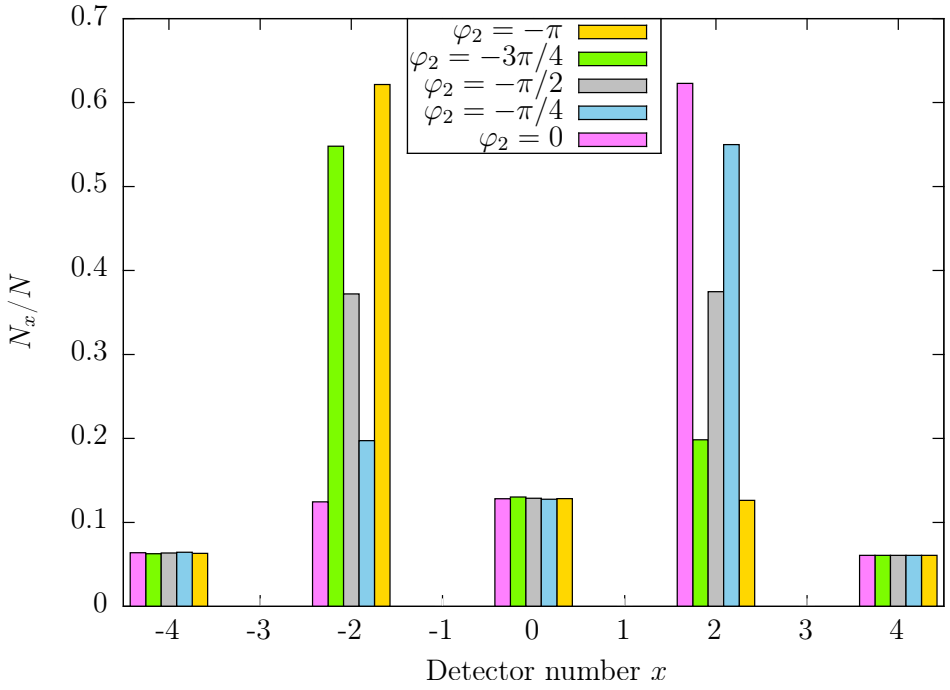

Figure 4.11: Dependence of the simulated distribution N_x/N on the detector number x for the 4-level quantum walk for various angles φ_2 and $\varphi_1 = \pi/2$.

From the analytical calculation, we expect the simulation results to depend only on φ_2. To investigate the dependence of the simulated distributions N_x/N on the angles φ_1 and

φ_2, we run the simulation with different values for these angles. The results when varying φ_1 are shown in Fig. 4.10, and the results when varying φ_2 can be seen in Fig. 4.11. From Fig. 4.10 it is seen that the simulated distribution of the 4-level quantum walk does not depend on φ_1. Results for different numbers of levels show the same behavior (results not shown). This finding agrees with the analytical result (see Table 4.2). In Fig. 4.11, a clear dependence of the simulated distribution on the angle φ_2 is seen. For $\varphi_2 = -\pi/2$ the distribution is symmetric. With increasing (decreasing) values for φ_2 the distribution becomes asymmetric with a peak on the left (right). These results show that varying the angle φ_2 suffices to reproduce both the symmetric and the different asymmetric quantum walk results obtained analytically. The variation of φ_1 does not change the outcome. Hence, the experimental setup could have been simplified by omitting the phase shifter with angle φ_1 and it would still produce the same results.

Investigating the mean and variance of the position x of the quantum walk, we find that the mean depends on φ_2 (see Fig. 4.12) and the variance grows faster than for the classical random walk, namely quadratically as visualized in Fig. 4.13.

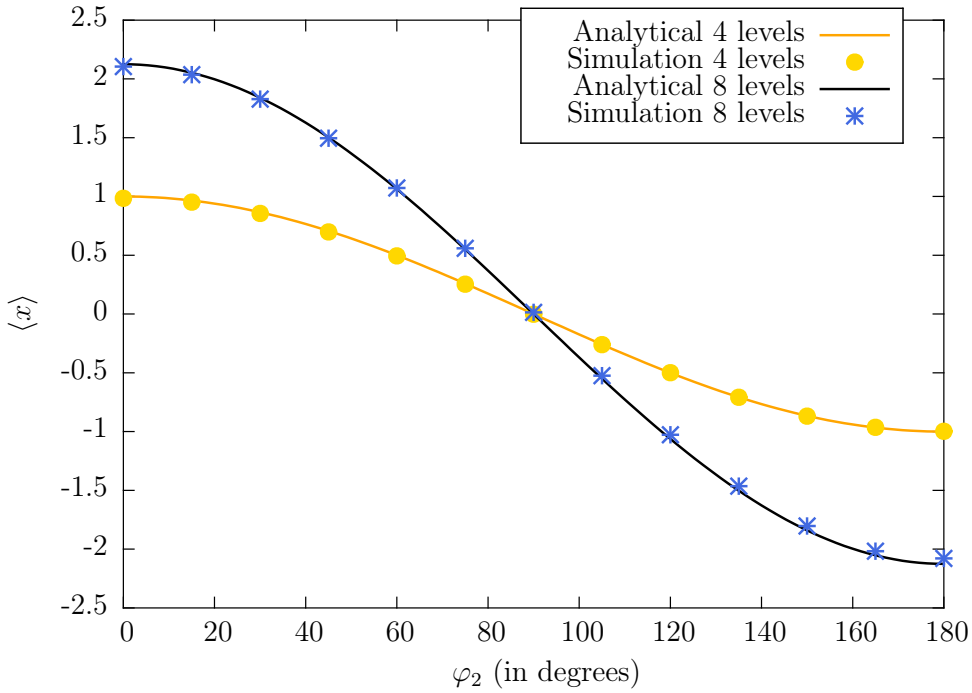

Figure 4.12: Mean of the position x of the quantum walk dependent on the angle φ_2. As an example, the 4-level and the 8-level quantum walk are shown with $N = 100\,000$ and $N = 200\,000$, respectively. Lines visualize the analytical results, dots and stars show the results from the simulation. For $\varphi_2 \neq \pi/2$, the mean differs from zero which is the mean of the random walk.

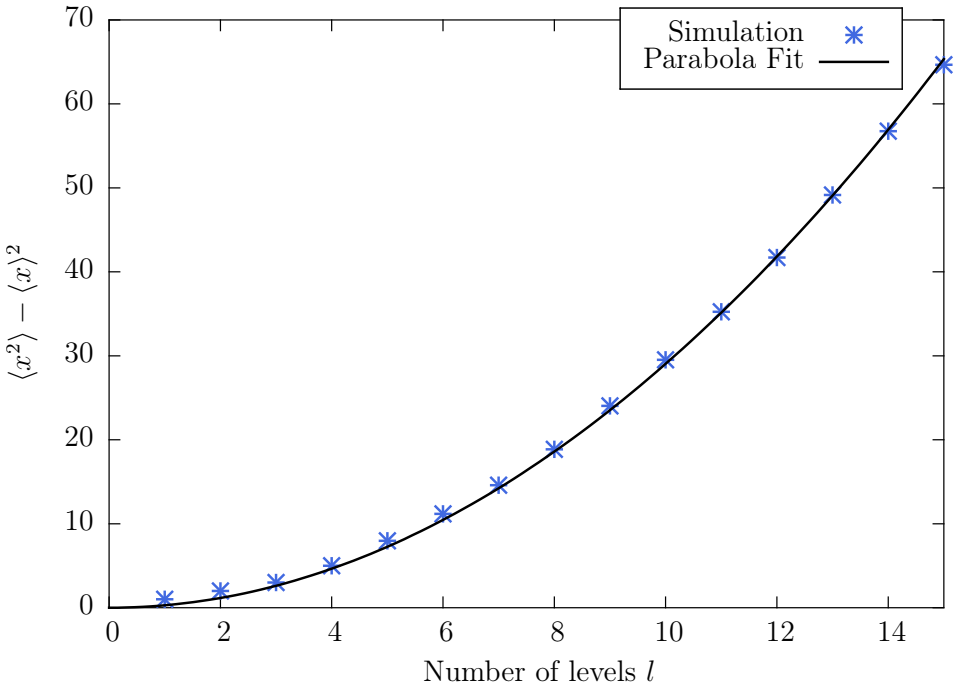

Figure 4.13: Variance of the position x of the symmetric quantum walk dependent on the number of levels l. Blue stars come from the simulation and the black line is a fitted parabola of the from ax^2 as the variance is expected to be zero for zero levels due to the preparation. The parameter a is determined to be $a = 0.290 \pm 0.001$. Obviously, the variance grows quadratically, which is different from the classical random walk.

Conclusion

Summarizing the results of the discrete-event simulation of the quantum walk, we can say that we are able to reproduce the distributions of a quantum walk of an arbitrary number of levels by means of the suggested experimental setup introduced in Ref. [23]. We find that the analytical and the numerical results are in very good agreement. Furthermore, the angle φ_1 does not contribute to the shape of the distribution but φ_2 can be used to achieve symmetric and asymmetric distributions. The asymmetric ones lead to the mean of the position x being different from zero. Finally, we could determine the prefactor $a = 0.290 \pm 0.001$ of the parabola describing the growth of the variance of the position x of the quantum walk. The square root of this result $\sqrt{a} \approx 0.54$ is not far away from the number 0.6 given in Ref. [35] for the prefactor of the standard deviation of the quantum walk.

Now that we have investigated the basics of the quantum walk, we discuss and simulate, in the following sections, an experiment which uses the quantum walk to show a violation of the so called Leggett-Garg inequality [24]. First, we have a look at the Leggett-Garg inequality itself, then we simulate the experiment by utilizing a discrete-event simulation, and finally we discuss the results and compare them with the experiment to see whether the quantum walk really violates the Leggett-Garg inequality.

4.2.2 Leggett-Garg Inequality

In Ref. [41], Leggett and Garg derive an inequality for correlations $K_{ij} = \langle Q_i Q_j \rangle$ of quantities Q_i measured at times t_i which can attain the values ± 1. For their derivation Leggett and Garg assume "macroscopic realism" and "non-invasive measurability" which they denote by (A1) and (A2), respectively. From (A1), they conclude that for an ensemble of systems prepared in some way at time t_0, joint probability densities like $\rho(Q_1, Q_2)$, $\rho(Q_1, Q_2, Q_3)$ $(t_0 < t_1 < t_2 < t_3)$ and correlation functions K_{ij} can be defined. Moreover, these "probability densities must be consistent" such that the following relations hold [41]:

$$\begin{aligned} \sum_{Q_1=\pm 1} \rho(Q_1, Q_2, Q_3) &= \rho(Q_2, Q_3) \\ \sum_{Q_2=\pm 1} \rho(Q_1, Q_2, Q_3) &= \rho(Q_1, Q_3) \\ \sum_{Q_3=\pm 1} \rho(Q_1, Q_2, Q_3) &= \rho(Q_1, Q_2). \end{aligned} \tag{4.12}$$

So they say, given Eq. (4.12), that it is possible to measure only pairs of Q_1, Q_2, and Q_3 in an experiment, and get the same results as if the complete triple was measured. Assuming that Eq. (4.12) is satisfied, one can indeed derive (see Ref. [42]) the inequality

$$\langle Q_1 Q_2 \rangle + \langle Q_2 Q_3 \rangle - \langle Q_1 Q_3 \rangle \leq 1, \tag{4.13}$$

where

$$K_{ij} = \langle Q_i Q_j \rangle = \sum_{Q_i=\pm 1} \sum_{Q_j=\pm 1} Q_i Q_j \rho(Q_i, Q_j) \tag{4.14}$$

is computed from pairs only. If Eq. (4.12) is not fulfilled, however, one has to use

$$K_{ij} = \sum_{Q_1=\pm 1} \sum_{Q_2=\pm 1} \sum_{Q_3=\pm 1} Q_i Q_j \rho(Q_1, Q_2, Q_3). \tag{4.15}$$

In an experiment, K_{ij} can be calculated from the measurement outcomes of N repetitions as $K_{ij} = \sum_{\alpha=1}^{N} Q_{i,\alpha} Q_{j,\alpha}/N$, where in each repetition α, the quantities Q_1, Q_2, and Q_3 must be measured. Then one can use the inequality

$$Q_1 Q_2 + Q_2 Q_3 - Q_1 Q_3 \leq 1, \tag{4.16}$$

which holds for each triple measured in a single run of an experiment, to derive Eq. (4.13) for the expectation values of the correlations:

$$\langle Q_1 Q_3 \rangle = \frac{1}{N} \sum_{\alpha=1}^{N} Q_{1,\alpha} Q_{3,\alpha} \geq \frac{1}{N} \sum_{\alpha=1}^{N} (Q_{1,\alpha} Q_{2,\alpha} + Q_{2,\alpha} Q_{3,\alpha} - 1) = \langle Q_1 Q_2 \rangle + \langle Q_2 Q_3 \rangle - 1. \tag{4.17}$$

Here, the requirement of measuring the triple and not only pairs is essential such that in an experiment, Q_1, Q_2, and Q_3 have to be measured in a single run if Eq. (4.12) is not fulfilled.

Summarizing these important remarks on the Leggett-Garg inequality, one can say that the Leggett-Garg inequality is always satisfied if triples are measured. If only pairs are measured and Eq. (4.12) does not hold, it can be violated.

4.2.3 Investigation of a Quantum Walk Experiment Violating the Leggett-Garg Inequality

Robens *et al.* present in their paper [24] an experiment with cesium atoms in a state-dependent lattice potential to produce the outcome of a 4-level quantum walk. They make use of two internal hyperfine states of the electronic ground state, $|F = 4,\, m_F = 4\rangle$ and $|F = 3,\, m_F = 3\rangle$, of the cesium atom which then experience different lattice potentials. A microwave pulse prepares the atom in a superposition of these two states and another operation moves the atom one lattice site to the left or the right if the atom is in the state $|F = 4,\, m_F = 4\rangle$ or $|F = 3,\, m_F = 3\rangle$, respectively.

A slightly modified variant of this experiment can be simulated using the discrete-event simulation method. In the simulation, the atoms are replaced by photons of which the horizontal ($|H\rangle$) and vertical ($|V\rangle$) polarizations represent the two states of the atoms. The operations on the atoms are replaced by analogous operations on the photons using the optical elements introduced in chapter 2.

In order to mimic the separation of the two states of the atom in the experiment, we make use of polarizing beam splitters to separate the horizontally and vertically polarized photons. The polarizing beam splitters are arranged as shown in Fig. 4.14. For the creation of the superposition of the states, Hadamard transformations, i.e., half-wave plates combined with phase shifters by $\pi/2$ (see section 2.4), are inserted as depicted in Fig. 4.14. This simple setup however cannot yet lead to the expected results of a quantum walk because interference is missing. In the simulation based on the polarization of photons, an extra transformation will be necessary to include interference.

Using the notation that the vector $|k\rangle$ is directed to beam splitter k as visualized in Fig. 4.14 by the gray dashed lines, the description is close to the mathematical description used in section 4.2.1. For the analytical calculation of the probabilities of detection events at the various detectors, taking into account the actions of the polarizing beam splitters and the Hadamard transformations, and a simple addition of the vectors is already sufficient:

$$
\begin{aligned}
(SR)^4\,|H,0\rangle &= (SR)^3\,S\frac{|V,0\rangle - |H,0\rangle}{\sqrt{2}} \\
&= (SR)^3\,\frac{|V,1\rangle - i|H,-1\rangle}{\sqrt{2}} \\
&= (SR)^2\,S\frac{|V,1\rangle + |H,1\rangle - i|V,-1\rangle + i|H,-1\rangle}{2} \\
&= (SR)^2\,\frac{|V,2\rangle + i|H,0\rangle - i|V,0\rangle - |H,-2\rangle}{2} \\
&= (SR)\,S\frac{|V,2\rangle + |H,2\rangle - 2i|H,0\rangle - |V,-2\rangle + |H,-2\rangle}{2\sqrt{2}} \\
&= (SR)\,\frac{|V,3\rangle + i|H,1\rangle + 2|H,-1\rangle - |V,-1\rangle + i|H,-3\rangle}{2\sqrt{2}} \\
&= S\frac{|V,3\rangle + |H,3\rangle - i|H,1\rangle + i|V,1\rangle - 3|H,-1\rangle + |V,-1\rangle - i|H,-3\rangle + i|V,-3\rangle}{4} \\
&= \frac{|V,4\rangle + i|V,2\rangle + i|H,2\rangle + |V,0\rangle + |H,0\rangle + i|V,-2\rangle - 3i|H,-2\rangle + |H,-4\rangle}{4}
\end{aligned}
\tag{4.18}
$$

where

$$R = \frac{1}{\sqrt{2}}\Big(|V\rangle\langle V| - |H\rangle\langle H| + |V\rangle\langle H| + |H\rangle\langle V|\Big) \otimes \sum_k |k\rangle\langle k| \tag{4.19}$$

represents the rotation of the polarization, i.e., the Hadamard transformation, and

$$S = \sum_k \Big(|V, k+1\rangle\langle V, k| + i|H, k-1\rangle\langle H, k|\Big) \tag{4.20}$$

describes the polarizing beam splitter. Calculating the absolute values squared at each position to obtain the probability $P(x)$ for detector number x gives: $P(-2) = 1/16$, $P(-1) = 5/8$, $P(0) = 1/8$, $P(1) = 1/8$, and $P(2) = 1/16$. This is the expected distribution of a 4-level quantum walk (see also table 4.2 for $\varphi_2 = 0$ but note that the labeling of the detectors is different).

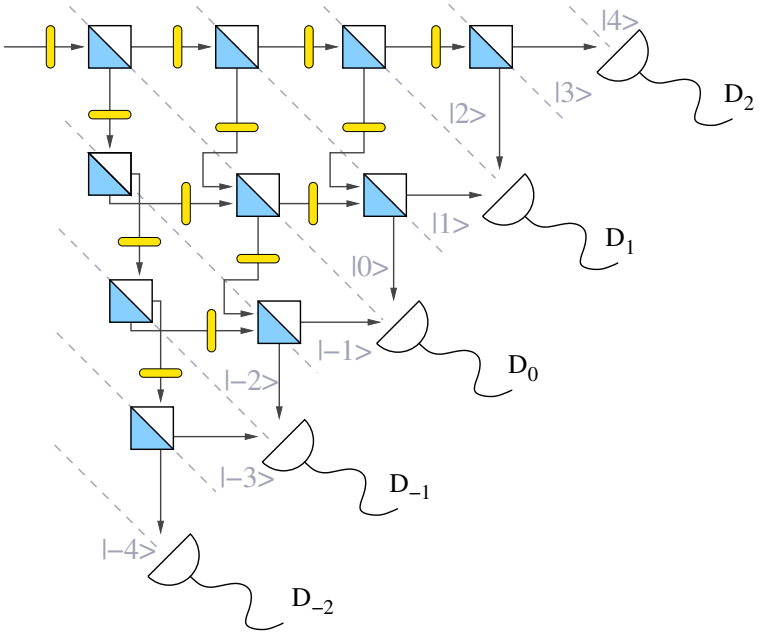

Figure 4.14: Setup in which the atom state transformations from the experiment in Ref. [24] are translated into optical elements. Blue-white boxes represent polarizing beam splitters which transmit vertically polarized light, and reflect horizontally polarized light. White half-circles with a tail denote detectors. Note: The labeling of the detectors is different from the one used in section 4.2.1 due to different labeling procedures in Refs. [23] and [24]. Gray dashed lines accompanied by a number visualize the naming of the vectors of the analytical calculation. The yellow boxes denote Hadamard transformations, corresponding to half-wave plates with angle $\vartheta = \pi/8$ followed by a phase shift of $\pi/2$. The incoming beam consists of horizontally polarized photons. This setup is not yet sufficient for the simulation of a quantum walk as interference, which happens naturally in the atom experiment, is lacking and therefore has to be considered additionally in the photon simulation.

As horizontally and vertically polarized photons do not interfere, in the simulation, interference has to be realized by an extra device. Examining each step of the analytical

calculation, we find that the addition of the vectors, which is easily done in the analytical calculation, is missing in the simulation. Interpreting the addition of the vectors in the physical setup of beam splitters and modes suggests that we have to put two photons with orthogonal polarizations, coming from different modes, into the same mode in order to get the required effect. A device performing exactly this process, and therefore being a suitable device to induce the interference, is the polarizing beam splitter, as it cannot only separate but also unite two modes. The required functionality of the polarizing beam splitter is illustrated in Fig. 4.15 for clarity. So instead of considering only a polarizing beam splitter followed by a Hadamard transformation on the polarization, we add a second polarizing beam splitter before the Hadamard transformation. The final setup for the quantum walk with horizontally and vertically polarized photons is shown in Fig. 4.16. Although half of the polarizing beam splitters seem unnecessary in the upper line, we put them there such that all components of the setup consist of the same elements just like in the experiment.

This setup indeed produces the expected result of the asymmetric 4-level quantum walk as illustrated in Fig. 4.18 by the yellow bars. So the quantum walk can also be reproduced by making use of the polarization of photons, which is also suggested in Ref. [43] with a slightly different scheme.

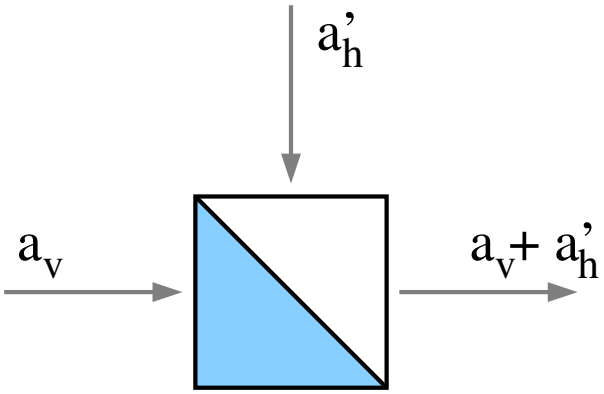

Figure 4.15: Sketch of the addition of vertically polarized light in the mode a and horizontally polarized light in the mode a' in a polarizing beam splitter. Since the polarizing beam splitter reflects horizontally polarized light but transmits vertically polarized light, both modes a and a' end up in the same output mode.

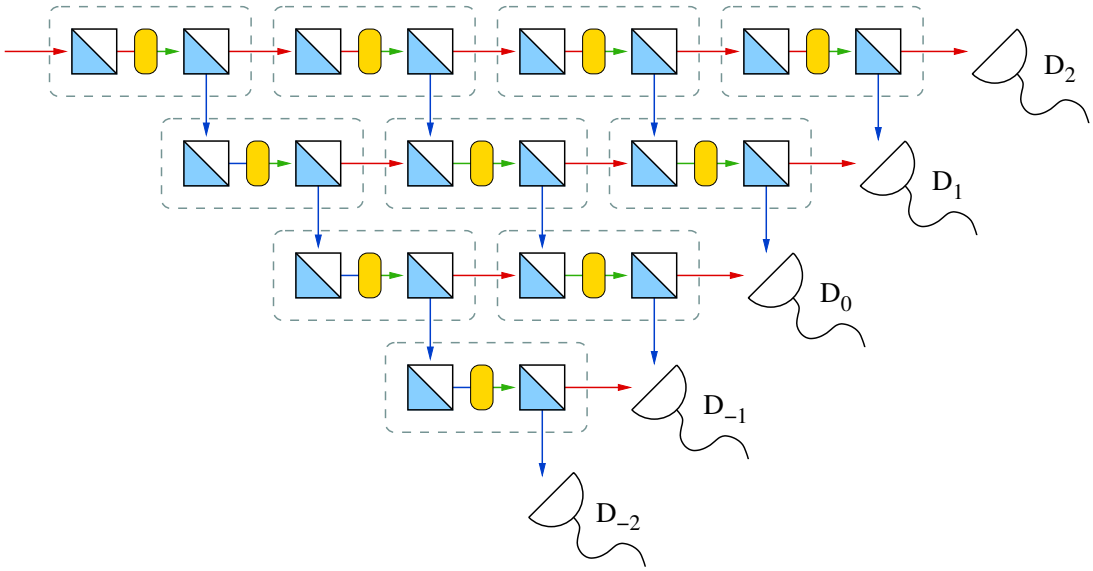

Figure 4.16: Setup for the quantum walk with polarized single photons as it is used in the discrete-event simulation. Blue-white boxes represent polarizing beam splitters transmitting vertically polarized light and reflecting horizontally polarized light. The yellow boxes denote the Hadamard transformation on the polarization, i.e., a half-wave plate followed by a phase shifter. Red lines illustrate vertically polarized photons, blue lines visualize horizontally polarized photons, and green lines depict superpositions of vertically and horizontally polarized light. The input beam consists of horizontally polarized photons. In this experiment, the source emits monochromatic light without fluctuations.

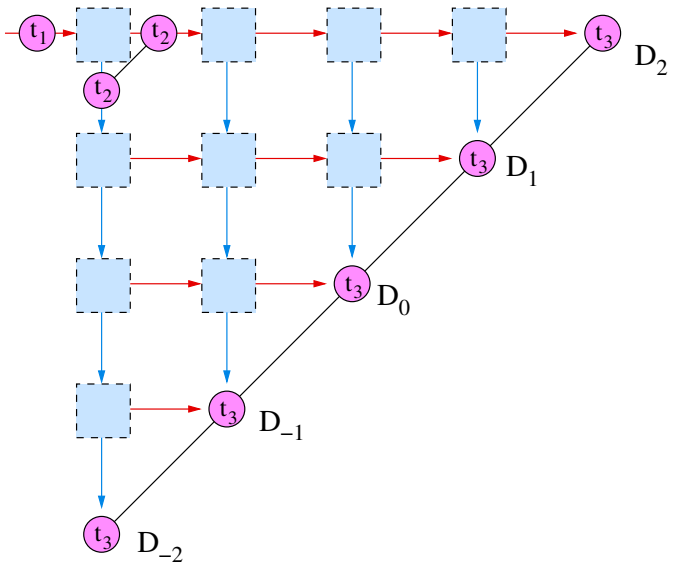

Figure 4.17: Sketch of the setup shown in Fig. 4.16 with the pink circles denoting at which positions and at which times a measurement takes place. The light blue boxes represent the elements encircled with the dashed gray lines in Fig. 4.16. The connecting lines between the pink circles illustrate that the corresponding measurements are performed at the same times.

Robens *et al.* show in Ref. [24] that their experiment violates the Leggett-Garg inequal-

ity

$$K = \langle Q(t_2)Q(t_1)\rangle + \langle Q(t_3)Q(t_2)\rangle - \langle Q(t_3)Q(t_1)\rangle \leq 1 \tag{4.21}$$

where the $Q(t_i)$ are real numbers with $|Q(t_i)| \leq 1$ and t_i denote the times at which a measurement is performed. The times t_i are indicated in Fig. 4.17 by pink circles within the sketch of the setup. In the experiment, $Q(t_1)$ is set to $Q(t_1) = 1$ as Robens *et al.* define the state preparation as their first measurement of the state. The time t_2 is after the first splitting, and there the position of the atom is measured. The two possible outcomes are then ± 1. Independently of the outcome, they set $Q(t_2) = 1$. The third measurement is a x-position measurement after the 4-th level of the quantum walk and $Q(t_3)$ is defined as

$$Q(t_3) = \begin{cases} -1 & \text{if outcome } x \leq 0 \\ 1 & \text{if outcome } x > 0. \end{cases} \tag{4.22}$$

Due to these choices, $\langle Q(t_2)Q(t_1)\rangle = 1$ and $\langle Q(t_3)Q(t_1)\rangle = \langle Q(t_3)\rangle$ such that Eq. (4.21) simplifies to

$$K = 1 + \langle Q(t_3)Q(t_2)\rangle - \langle Q(t_3)\rangle \leq 1. \tag{4.23}$$

In order to obtain $\langle Q(t_3)\rangle$ the average of the measured outcomes of $Q(t_3)$ for a fixed number of repetitions can be computed. In order to calculate $\langle Q(t_3)Q(t_2)\rangle$, Robens *et al.* use two additional runs of the experiment (including also a fixed number of repetitions). So they measure the position at t_2 by an ideal negative measurement and reject those atoms that are measured at position -1 $(+1)$ in the second (third) run. Atoms which are not rejected continue their way and are then measured at t_3. The average over the remaining outcomes of $Q(t_3)$ is then denoted by $\langle Q(t_3)\rangle_{x_2}$ where $x_2 \in \{-1, 1\}$ indicates which atoms are not rejected at t_2. The left-hand side of the Leggett-Garg inequality is then computed by Robens *et al.* as

$$K = 1 + \sum_{x_2=\pm 1} P(x_2;\, t_2)\langle Q(t_3)\rangle_{x_2} - \langle Q(t_3)\rangle \tag{4.24}$$

where $P(x_2;\, t_2)$ denotes the probability that the atom was at position x_2 at t_2. The value they finally compute for K (for the *fair coin toss*) is [24]

$$K = 1.435 \pm 0.074 > 1. \tag{4.25}$$

To reproduce this result, we run our discrete-event simulation program for the 4-level quantum walk three times. In the first run, we compute $\langle Q(t_3)\rangle$ without selecting the photons at level 2. The number of repetitions in the simulation is set to $N = 100\,000$. For the other two runs, we reject the photons traveling to the left or the right at level 2, respectively, like Robens *et al.* do in their experiment with the atoms. Then we compute K as given in Eq. (4.24) from three separate runs. Doing this with different seeds for the PRNG gives on average

$$K = 1.4966 \pm 0.0051 > 1 \tag{4.26}$$

The result obviously violates the Leggett-Garg inequality and is even close to the theoretical maximum of $K = 1.5$ achievable with this type of experiment [24]. The distributions gained from the three runs are shown in Fig. 4.18.

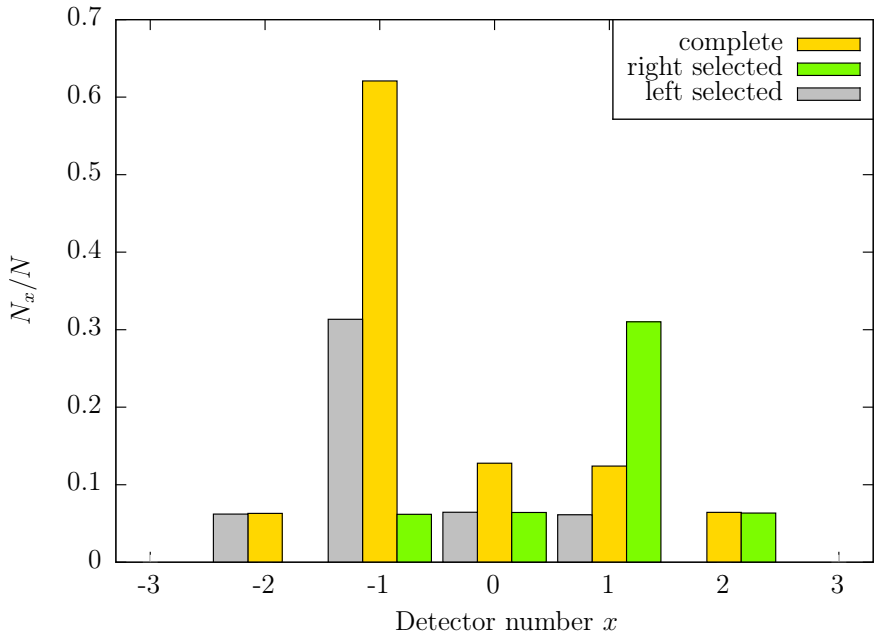

Figure 4.18: Results of the normalized number of detector counts N_x/N as a function of the detector number x obtained by the discrete-event simulation based on the procedure of the experiment. The number of repetitions for each of the three runs is $N = 100\,000$. The yellow bars represent the distribution of the 4-level quantum walk without any selection. The green (gray) distribution shows the outcomes if the photons leaving the first beam splitter to the left (right) are rejected. The distributions coincide with those presented in Ref. [24].

To verify that the Leggett-Garg inequality holds for the classical random walk, we compute the three components of K in three separate runs, i.e. in the same manner as for the quantum walk, but by using the simulation of the classical random walk discussed in section 4.1. The mean of the result for K using the classical random walk with different seeds is determined to be

$$K_{\text{class}} = 0.996 \pm 0.010, \tag{4.27}$$

which is very close to one. So for the classical random walk we obtain $K \approx 1$ with only statistical fluctuations. Indeed, the Leggett-Garg inequality holds in the classical case since no violation (apart from the statistical fluctuations) could be achieved. This is to be expected as for the classical random walk Eqs. (4.12) hold.

As we just demonstrated, the Leggett-Garg inequality can also be violated by a classical simulation of the quantum walk in which the position of the particle is always well-defined. The important question is now, whether the inequality is still violated if no particles are rejected, i.e. the particles' positions at t_2 are stored for a single run with N repetitions, and K is computed from this data only. The advantage of the simulation is that this non-invasive "measurement" at t_2 can be easily carried out, while it is not accessible in a real experiment. The difference in the outcomes of these two ways to "measure" the positions at t_2 can be seen in Fig. 4.19. This data, gained from single runs with different seeds for the random number generator, yields

$$K = 0.9999 \leq 1, \tag{4.28}$$

which means that the Leggett-Garg inequality is not violated if the correlations of the pairs are computed from one data set only and not from three different ones. Since this is the only thing that changed between those two computations, it is not the quantum walk itself which is "incompatible with well-defined, classical trajectories", as stated in Ref. [24].

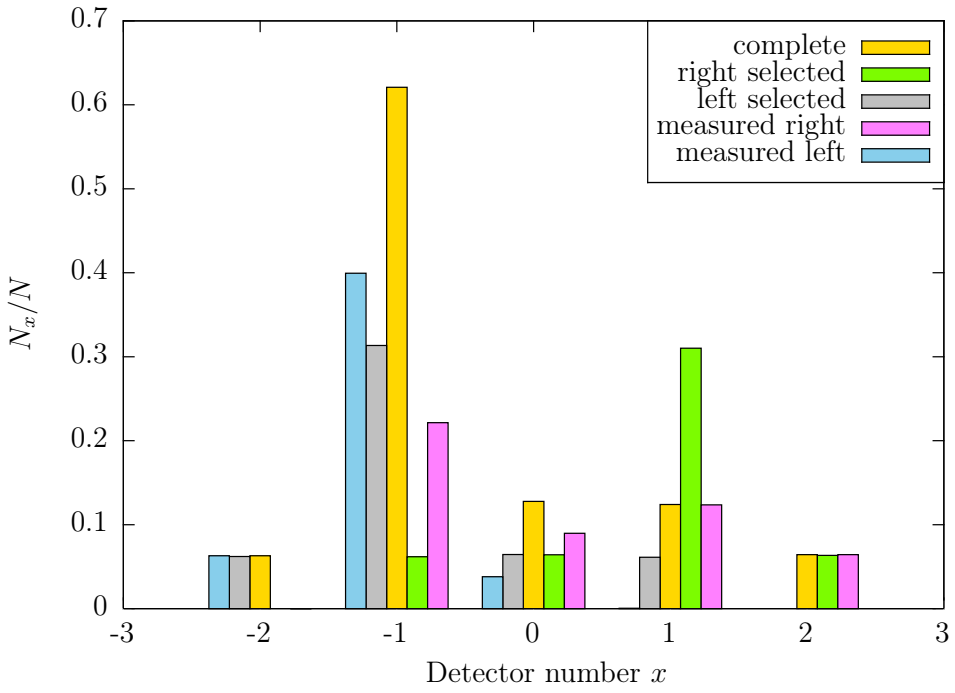

Figure 4.19: Comparison of the results of the normalized number of detector counts N_x/N as a function of the detector number x for two versions of the quantum walk experiment: The green and gray bars illustrate the distributions obtained by rejecting the left or the right going part of the particles, respectively, and the blue and pink distributions show the outcomes where the positions at t_2 are stored but the particles are not rejected. Obviously, the distributions are not the same. The yellow bars show the distribution of the quantum walk without selection.

Conclusion

Summarizing the results of this analysis, we can reproduce the results of the quantum walk, and likewise the outcome of the experiment of Robens *et al.* including the violation of the Leggett-Garg inequality, with a discrete-event simulation of photons where the state of the atoms in the original experiment is replaced by the polarization of the photons. Moreover, we are able to simulate a really non-invasive measurement such that we can reduce the three runs needed in the experiment to a single run providing all necessary data. Evaluating this data set yields that the Leggett-Garg inequality is not violated.

Supported by the results of this investigation, we state that one can only conclude that quantum mechanics violates assumption (A2), i.e. non-invasive measurability, since a measurement in an experiment cannot be performed non-invasively as it can be done in the simulation. The simulation however is event-based, i.e., the simulated particle always has a well-defined position and therefore obeys (A1), the macroscopic realism. Nevertheless, it is possible to violate the Legett-Garg inequality in the same way as done

in the experiment. Making use of the advantage of really non-invasive measurability in the simulation leads to the Leggett-Garg inequality being satisfied. The reason why this experiment leads to a violation of the Leggett-Garg inequality is that the measurement at time t_2 is still invasive. Although Robens *et al.* claim their measurement is non-invasive, they still need three runs of the experiment. This is because they can never measure triples but only pairs. The measurement at t_2 leads to

$$\sum_{x_2=\pm 1} \rho(x_1, x_2, x_3) = \rho(x_1, x_3) \tag{4.29}$$

not being satisfied since the rejection of the photons being at the "wrong" position after the measurement leads effectively to an addition of the outcomes (i.e. modulus squared) of two 3-level runs shifted to the left and right, respectively, instead of the outcome of the 4-level quantum walk. The distribution of two added 3-level quantum walks (left hand side of Eq. (4.29)) obviously differs from the distribution of the 4-level run (right hand side) such that Eq. (4.29) cannot be satisfied in this experiment. So the selection at t_2 changes the initial state, i.e. the outcome of the first measurement. This is why in the second and third run, measurements take place effectively only at t_2 and at t_3. Obviously, in the first run, measurements are only at t_1 and at t_3. Removing particles at time t_2 changes the probability densities for the measurement at t_3. Therefore, Robens *et al.* cannot measure triples in a single run and the Leggett-Garg inequality can be violated just because of the invasive character of the measurement.

So it is sufficient that Eq. (4.29) is not fulfilled in the experiment for the Leggett-Garg inequality to be violated. However, measuring all three values in one run (simulation), the inequality holds which means that invasive measurement already suffices to make Eq. (4.29) invalid, since the Leggett-Garg inequality can be forced to be violated even with the discrete-event simulation. Therefore, one cannot conclude from a violation of the Leggett-Garg inequality that the system does not obey macroscopic realism, i.e. the particle does not have a well-defined state. The only conclusion which can be drawn is that in this experiment non-invasive measurability was not achieved, which is enough to cause a violation of the Leggett-Garg inequality. A similar, mathematical argument concerning violations of the Leggett-Garg inequality is also given in Ref. [44].

5 Cryptography

In this chapter, we will focus on cryptographic problems. We start with classical cryptography (where *classical* here means the current, non-quantum technology), and then proceed to quantum key distribution, where we will especially consider the so-called BB84 protocol and simulate an experiment based on further development of this protocol.

Already in ancient times people encrypted their secret messages when sending them through an untrustworthy deliverer to the recipient, or in case the sender got attacked such that not everyone able to read was also able to read the secret message. Nowadays things have changed, but still we have to encrypt our messages when we send them via a public channel like a telephone line or the internet and we do not want everybody to read them. There are many different cryptographic protocols with various advantages and disadvantages, and therefore they are not all equally well suited for all cryptographic purposes.

In the following we first have a look at a few classical, currently used cryptosystems, and then we discuss in more detail quantum key distribution where quantum physics is used to implement cryptographic protocols. But before we start with the description of classical cryptosystems, we have to introduce the basic terminology including the definition of a cryptosystem.

5.1 Classical Cryptography

Definitions and Terminology

When talking about cryptography, the sender is usually called Alice and the recipient is called Bob. A third party adversary, often an eavesdropper called Eve, is to be prevented from reading a secret message on the public channel. Alice aims at hiding the message from Eve but making it still readable to Bob. She has to encrypt her secret message such that only Bob is able to decrypt it. For this purpose, they have to agree on a cryptosystem and a key. This system is mathematically defined as follows:

A *cryptosystem* $(\mathcal{M}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ consists, according to Ref. [45], of a finite set $\mathcal{M}$ of all possible *messages* or *plaintexts* m, a finite set $\mathcal{C}$ of all possible *ciphertexts* c, a *key space* $\mathcal{K}$ which is a finite set of all possible *keys* k, a set $\mathcal{E}$ of encryption functions

$$e_k : \mathcal{M} \to \mathcal{C} \qquad \text{for each } k \in \mathcal{K}, \tag{5.1}$$

and a set $\mathcal{D}$ of decryption functions

$$d_k : \mathcal{C} \to \mathcal{M} \qquad \text{for each } k \in \mathcal{K}. \tag{5.2}$$

The encryption and the decryption functions have to fulfill certain criteria. The most important and obvious criterion is that $d_k(e_k(m)) = m$ for all $m \in \mathcal{M}$, $k \in \mathcal{K}$ since Bob should be able to decrypt any message Alice might send. Moreover, $e_k(m)$ and $d_k(c)$

should be easy to compute, i.e., there should be efficient algorithms to compute $e_k(m)$ and $d_k(c)$ for known k such that the computations do not take a long time. However, solving $c = e_k(m)$ or $m = d_k(c)$ for k should be infeasible for all cryptosystems where the key k is reused, so that Eve cannot retrieve the key from an intercepted ciphertext-message pair for all following communications between Alice and Bob. The set of functions e_k and d_k is also called *cipher*.

Ideally, the encryption functions return a ciphertext c which reveals no information about the original plaintext m to anyone who does not have the corresponding key k. Many cryptosystems do not satisfy this criterion but they are nevertheless considered *provably secure* cryptosystems, i.e., it can be proven that breaking the system is at least as hard as solving, e.g., a problem in the class NP (non-deterministic polynomial) that is assumed not to be in the class P (polynomial), such as factoring. However, since NP $\neq$ P has not yet been proven, this statement still relies on assumptions of computational hardness [45].

A cryptosystem is defined to have *perfect secrecy* if $P(\hat{m} = m) = P(\hat{m} = m \,|\, \hat{c} = c)$. This means, the probability that the plaintext is m is equal to the conditional probability that the plaintext is m given that the ciphertext c is observed, for all $m \in \mathcal{M}$, $c \in \mathcal{C}$ [45]. If a cryptosystem can be proven to have perfect secrecy, it is *unconditionally secure*, i.e., even if Eve has access to infinite computational power, she cannot break the system. A necessary condition for perfect secrecy is that there have to be at least as many possible keys as there are possible plaintexts [45]. This implies that the key must not be shorter than the plaintext, which is an impractical condition as then sharing a secret key ad hoc is at least as difficult as sending the message securely. A cipher that has perfect secrecy is the one-time pad which, among others, will be discussed in the next section.

There are two kinds of cryptosystems, *symmetric* and *asymmetric* cryptosystems. For a symmetric cryptosystem, the encryption and decryption is symmetric, i.e., the same key is used for encryption and decryption. Hence, the two parties Alice and Bob have to share the same key in order to use a symmetric cryptosystem. This is why symmetric ciphers have the disadvantage of key management: The key has to be distributed in advance and kept secret until it is needed. Moreover, each communicating pair needs its own secret key, resulting in the number of required keys growing quadratically [46].

Asymmetric cryptosystems employ different keys for the encryption and decryption. The decryption key of the recipient has to be kept private, but the key for encryption can be made public. Thus, anybody is able to encrypt a message, but only the legitimate recipient can decrypt and read it. This is comparable to a mailbox where everyone can put in a message, but only the owner can open the mailbox and read the messages [47]. For that reason, asymmetric cryptosystems are called *public-key cryptosystems* and were first proposed by Diffie and Hellman in 1976 [46] as a solution for the above-mentioned disadvantages of symmetric cryptosystems. For systems of this kind, Bob possesses a pair of keys, namely a *private key* k_d for decryption and a *public key* k_e for encryption.

A Survey of Selected Classical Cryptosystems

Examples of currently popular, and therefore often used, cryptosystems are AES [48] (the Advanced Encryption Standard) as a symmetric cipher and RSA (after the inventors Rivest, Shamir, and Adleman) [49] as a public-key cryptosystem.

AES is a block cipher, meaning that the message is split up into blocks of a fixed length l, and each of these blocks is encrypted separately. Therefore, it is quite fast and can

be used for large amounts of data especially on parallel architectures. For block ciphers, there exist different modes of operation that combine consecutive blocks to prevent blocks of length l containing the same data from being revealed. This can be a problem for encrypted images [50].

For RSA, calculations are performed in a finite multiplicative group $\mathbb{Z}_n$ where $n \in \mathbb{N}$ is different for each user. This means that every message has to be represented as a number $m \in \mathbb{Z}_n$. Apart from that, each user has his own keys $k_d = D_B$ and $k_e = (E_B, n_B)$ where $E_B \cdot D_B \equiv 1 \pmod{(p_B - 1)(q_B - 1)}$, p_B, q_B prime with $p_B \cdot q_B = n_B$ (the subscript B denotes that the variables are special for each user, here Bob). When Alice wants to send a secret message m to Bob, she does not need her own key but she can use Bob's public key k_e to encrypt her message m to the ciphertext

$$c \equiv m^{E_B} \pmod{n_B}, \tag{5.3}$$

and then send it to Bob. He, in turn, is the only one that can decrypt the message by applying the private key k_d to the ciphertext:

$$c^{D_B} \equiv m^{E_B \cdot D_B} \equiv m^{E_B \cdot D_B \pmod{(p_B-1)(q_B-1)}} \equiv m^1 \equiv m \pmod{n_B}. \tag{5.4}$$

For more details on number theory regarding RSA see, for example, Ref. [49]. Eve can have the public key (E_B, n_B), but she cannot use it to decrypt the message immediately or to recover the private key D_B as this would require factoring $n_B = p_B q_B$. The advantage of this scheme is that Alice and Bob do not have to share a secret key in advance and the number of required keys grows only linearly in the number of users. As the computation of the encryption and decryption is expensive compared to those of a symmetric cipher and therefore not suited for the encryption and decryption of large amounts of data, RSA is often used for small amounts of data or to distribute a key for a symmetric cipher like AES. Another advantage is that a slight modification of this cryptosystem also gives a signature scheme to sign messages digitally [49]. So if Alice also possesses a pair of private $(k_d = D_A)$ and public $(k_e = (E_A, n_A))$ keys, she can encrypt the message m with her private key first to the signature $s \equiv m^{D_A} \pmod{n_A}$ and then encrypt the pair $(m, s) =: o$ with Bob's public key $o^{E_B} \equiv c \pmod{n_B}$. Bob can then decrypt the ciphertext with his private key first $c^{D_B} \equiv o \equiv (m, s) \pmod{n_B}$ and, after that, decrypt s with Alice's public key: $s^{E_A} \equiv m_0 \pmod{n_A}$. If $m_0 = m$, Bob can be sure that the message was sent by Alice. Breaking the RSA cryptosystem can be proven to be at least as difficult as factoring [49].

The one-time pad, patented by Gilbert Vernam and therefore sometimes called Vernam cipher, is an example for a symmetric cryptosystem that has perfect secrecy if the key is truly random (pseudo random numbers that still show some structure are not satisfactory) and it is at least as long as the message. Furthermore, it has to be used only once [45]. So the key has to be generated by a real random number generator which takes some time, especially if long messages are to be encrypted. Transmission of such a key is also a problem, and since the key is not to be used more than once, transmission has to be done often. If the key is used more than once, decryption of the first ciphertext with the second ciphertext removes the key, and one ends up with the first message encrypted with the second message. As this data is not random but exhibits structures of the language, it is breakable. Moreover, if Eve is able to intercept a plaintext-ciphertext pair, she can easily obtain the key, and then she could read all the following communications between Alice and Bob. Encryption and decryption on the other side are quite simple: If we consider

a sequence of N bits $m_1 m_2 m_3 \dots m_N$ representing the message, encryption is done by XORing (exclusive-or operation $\oplus$) the N-bit message with the N-bit key $k_1 k_2 k_3 \dots k_N$:

$$c_i = m_i \oplus k_i, \quad \forall i = 1, 2, \dots, N \tag{5.5}$$

resulting in the N-bit ciphertext $c_1 c_2 c_3 \dots c_N$. Decryption is done equivalently by XORing the ciphertext with the key

$$c_i \oplus k_i = m_i \oplus k_i \oplus k_i = m_i, \quad \forall i = 1, 2, \dots, N \tag{5.6}$$

as $k_i \oplus k_i = 0$ for $k_i = 0$ or $k_i = 1$. Although the one-time pad has perfect secrecy and the encryption and decryption functions are easy to compute, the impractical handling of the key makes the one-time pad a rarely used cipher [45].

Although the security of RSA and many other public-key cryptosystems is based on the assumption that certain computational problems like factoring or computation of the discrete logarithm are hard (i.e., the number of operations grows exponentially in the number of bits) to solve on a (classical) computer, it is nowadays one of the most often used cryptosystems. But, besides the fact that the hardness of these problems is not proven for classical computers, another threatening problem is that on a quantum computer factoring (and computation of the discrete logarithm) can in principle be performed efficiently, i.e., in polynomial time as proven by Shor [21]. So if a sufficiently large quantum computer has been built, many currently used cryptosystems are not secure anymore. Although there are still (classical) cryptosystems that are resistant against a quantum computer like the unconditionally secure one-time pad, there is still the problem of performing key distribution without relying on public-key cryptosystems which are not (yet) proven to be resistant against the power of a potential quantum computer. In the following, we will therefore outline how quantum physics may provide a remedy in finding new secure and resistant techniques for key distributions.

5.2 Quantum Key Distribution

Since the invention of Shor's efficient factoring algorithm for a quantum computer [21], it has become evident that many of the currently used classical cryptosystems are not secure anymore once a sufficiently large quantum computer becomes available. On the other hand, there exists at least one cryptosystem, namely the one-time pad, which has perfect secrecy and is therefore unbreakable even for a quantum computer. The only problem is the sharing of the random, secret key that is as long as the message. That is where quantum physics comes in.

In 1984 Bennett and Brassard proposed a key distribution protocol [51] (later called BB84) for the one-time pad (but also applicable to other symmetric ciphers) based on the laws of physics. The BB84 protocol is the first cryptographic protocol making use of quantum mechanics in order to distribute a secret key ad hoc between two parties Alice and Bob. In the original paper [51], four polarization states of single photons serve as bits. The four polarization states consist of two orthonormal bases, the rectilinear and the diagonal basis which are conjugate, i.e., measuring a basis state of one basis in the other basis gives each result with equal probability. One state of each basis represents the bit "0" and the other one represents the bit "1". The bit sequence obtained by the BB84 protocol is random, and therefore only suited for key distribution but not for the transmission of

meaningful messages. The reason for this is that, in the end, only a random part of the bits originally sent by Alice contribute to the final bit sequence.

In the following, we will examine the BB84 protocol in more detail regarding the steps to be performed as well as the basic ideas of its security.

5.2.1 The BB84 Protocol

In this section, we give a brief description of how the BB84 protocol works. Two parties, Alice and Bob, want to use the one-time pad (or another symmetric cipher) for the encryption of their secret communication. They share an authenticated, classical public channel so that they know they are communicating with each other and not with Eve, and a quantum channel, but they do not share a secret key. They agree to use the BB84 protocol for the (quantum) key distribution that works as follows:

First, Alice has to generate a secret, random bit sequence of about twice the length they need for the message. Then she has to manipulate the polarization of the photons she wants to send to Bob. For each photon, she chooses at random either the rectilinear basis $\mathcal{R}$ (horizontal $|H\rangle$ and vertical $|V\rangle$ polarization) or the diagonal basis $\mathcal{D}$ (diagonal $|D\rangle$ and antidiagonal $|A\rangle$ polarization) where

$$|D\rangle = \frac{|V\rangle + |H\rangle}{\sqrt{2}} \quad \text{and} \quad |A\rangle = \frac{|V\rangle - |H\rangle}{\sqrt{2}}. \tag{5.7}$$

The encoding of the random bit sequence is done by preparing the photons according to the identifications

$$0 \mathrel{\hat{=}} |H\rangle \quad \text{and} \quad 1 \mathrel{\hat{=}} |V\rangle \tag{5.8}$$

or

$$0 \mathrel{\hat{=}} |D\rangle \quad \text{and} \quad 1 \mathrel{\hat{=}} |A\rangle, \tag{5.9}$$

respectively, at random. Then the photons are sent to Bob via the quantum channel.

Bob measures the polarizations of the photons arriving at his laboratory at random either in the rectilinear or in the diagonal basis. As he chooses the basis independently from Alice, they coincide in about one half of the choices. In these cases, Bob gets as measurement outcome the polarization Alice prepared. For example, if Alice prepares the state $|H\rangle$ and Bob measures in the rectilinear basis, the probabilities for his measurement outcomes horizontal H and vertical V are

$$P(V \,|\, H) = 0 \quad \text{and} \quad P(H \,|\, H) = 1. \tag{5.10}$$

In the other cases, his measurement outcome is totally random: If he measures in the diagonal basis, he gets the outcomes diagonal D and antidiagonal A with probabilities

$$P(D \,|\, H) = \big|\big||D\rangle\langle D|H\rangle\big|\big|^2 = 1/2 \tag{5.11}$$

$$P(A \,|\, H) = \big|\big||A\rangle\langle A|H\rangle\big|\big|^2 = 1/2, \tag{5.12}$$

respectively.

After Bob converts his measurement results into bits via the identifications given in Eq. (5.8) and Eq. (5.9), Alice and Bob have bit sequences which agree in about three

quarters of the bits. In order to obtain the exact same bit sequence, they have to discard those bits where they cannot be sure that they have the same without announcing the bit itself. For approximately one half of the bits, namely the ones they used the same basis for, they can find out whether their bits match by only announcing the basis they used. So Bob has to tell Alice by using the authenticated classical channel which bases he chose for the measurements, and Alice confirms the correct ones. If they used different bases, the corresponding bit is discarded. This is why Alice has to start with about twice as many bits as needed. So now Alice and Bob share the same secret bit sequence which they can use as a key for the one-time pad.

The security of the BB84 protocol relies on Heisenberg's uncertainty principle as described by Bennett *et al.* [52] but also on the no-cloning theorem [47], which was first mentioned in [53] and [54]. Due to the no-cloning theorem, the eavesdropper Eve cannot make a (reliable) copy of a quantum state. This is because a unitary transformation U such that

$$U\left(|\chi_1\rangle \otimes |a\rangle\right) = |\chi_1\rangle \otimes |\chi_1\rangle \tag{5.13}$$
$$U\left(|\chi_2\rangle \otimes |a\rangle\right) = |\chi_2\rangle \otimes |\chi_2\rangle, \tag{5.14}$$

where $|\chi_1\rangle$ and $|\chi_2\rangle$ are two arbitrary states to copy, and $|a\rangle$ is an ancilla qubit, does only work reliably if $|\chi_1\rangle$ and $|\chi_2\rangle$ are orthogonal [55], but for instance, $|H\rangle$ and $|D\rangle$ are not orthogonal. Thus, these states cannot be copied reliably by Eve such that storing the (to her unknown) state and measure it at a later time, e.g., after Alice and Bob announced their bases, becomes impossible for her. So she would have to act during the transmission process for example by using the intercept-resend method. But due to Heisenberg's uncertainty principle, she cannot simply measure the polarization, get the correct polarization independently of the basis, and send a new photon in the correct state to Bob. A measurement of the polarization in a basis conjugate to the one used by Alice gives both possible measurement outcomes with the same probability; so in about one half of the cases where she chose the conjugate basis, she will figure out the same bit as Alice but not the correct polarization state. So Eve would get a wrong result only in half the cases where she measured in the conjugate basis but would always send the wrong polarization state to Bob. So she could gain, on average, information on three quarters of the secret bits, namely those where she chose the correct basis, and one half of the bits where she chose the conjugate basis. However, due to her measurements in the conjugate basis, the polarization of the photon sent to Bob is according to her measurement outcome in the conjugate basis. This can lead to the detection of Eve if Alice and Bob measure in the same basis but Eve chose the conjugate one. Then the probability that the results of Alice and Bob do not match is $1/4$ (with probability $1/2$, Eve chooses the conjugate basis, and with probability $1/2$ Bob measures "0" or "1") although they used the same basis. Alice and Bob can take advantage of this fact by comparing some of their bits publicly and checking whether Eve caused disagreements by eavesdropping.

To compare some bits of their shared key to check for an eavesdropper, it is useful for Alice to generate a bit sequence which is even longer than twice the length needed. So the next step after the comparison of the basis would be to compare some randomly chosen bits of the key (about a third of the remaining ones [51]) using the classical channel. These bits have to be discarded as they are publicly announced. In the ideal case, all these compared bits should be the same. In case they are not equal, someone was eavesdropping on the quantum channel during the transmission. An example is given

in Table 5.1 without eavesdropping and in Table 5.2 with Eve using the intercept-resend method for eavesdropping.

In the realistic, non-ideal case, the polarization can change due to interaction of the photons with the environment or non-perfect alignment of the devices leading to bit flip errors, or photons are not detected at all by Bob due to losses in the channel or imperfect detectors. Usually, all disturbances (also those due to the environment) are ascribed to a potential eavesdropper, making him only appear more powerful such that he is not underestimated. Alice and Bob then have to estimate at which error rate it is still secure to use the key. For instance, if the eavesdropper was only able to gain very little information of the key, techniques such as error correction and privacy amplification, which was invented by Bennett, Brassard, and Robert in 1988 [56], are still sufficient [47]. Otherwise they have to abort the protocol.

Table 5.1: Example of the BB84 quantum key distribution protocol without eavesdropping in the ideal case.

Alice's bit	0	1	1	0	1	0	1	0	0	0	1	0	1	1	1	0	0	1
Alice's basis	$\mathcal{R}$	$\mathcal{D}$	$\mathcal{D}$	$\mathcal{R}$	$\mathcal{D}$	$\mathcal{R}$	$\mathcal{R}$	$\mathcal{D}$	$\mathcal{R}$	$\mathcal{D}$	$\mathcal{D}$	$\mathcal{D}$	$\mathcal{R}$	$\mathcal{D}$	$\mathcal{R}$	$\mathcal{R}$	$\mathcal{D}$	$\mathcal{R}$
Alice's state	H	A	A	H	A	H	V	D	H	D	A	D	V	A	V	H	D	V
Bob's basis	$\mathcal{R}$	$\mathcal{R}$	$\mathcal{D}$	$\mathcal{R}$	$\mathcal{D}$	$\mathcal{D}$	$\mathcal{D}$	$\mathcal{D}$	$\mathcal{R}$	$\mathcal{R}$	$\mathcal{R}$	$\mathcal{D}$	$\mathcal{R}$	$\mathcal{R}$	$\mathcal{R}$	$\mathcal{D}$	$\mathcal{R}$	$\mathcal{D}$
Bob's result	H	V	A	H	A	D	A	D	H	V	V	D	V	H	V	A	H	D
same basis	✓		✓	✓	✓			✓	✓			✓	✓		✓			
key	0		1	0	1			0	0			0	1		1			

Table 5.2: Example of the BB84 quantum key distribution protocol with Eve eavesdropping on the channel and using the intercept-resend method. As the third compared bit is incorrect in the ideal case, Alice and Bob can conclude that Eve was eavesdropping.

Alice's bit	0	1	1	0	1	0	1	0	0	0	1	0	1	1	1	0	0	1
Alice's basis	$\mathcal{R}$	$\mathcal{D}$	$\mathcal{D}$	$\mathcal{R}$	$\mathcal{D}$	$\mathcal{R}$	$\mathcal{R}$	$\mathcal{D}$	$\mathcal{R}$	$\mathcal{D}$	$\mathcal{D}$	$\mathcal{D}$	$\mathcal{R}$	$\mathcal{D}$	$\mathcal{R}$	$\mathcal{R}$	$\mathcal{D}$	$\mathcal{R}$
Alice's state	H	A	A	H	A	H	V	D	H	D	A	D	V	A	V	H	D	V
Eve's basis	$\mathcal{D}$	$\mathcal{D}$	$\mathcal{R}$	$\mathcal{R}$	$\mathcal{R}$	$\mathcal{D}$	$\mathcal{R}$	$\mathcal{D}$	$\mathcal{D}$	$\mathcal{R}$	$\mathcal{D}$	$\mathcal{R}$	$\mathcal{R}$	$\mathcal{D}$	$\mathcal{R}$	$\mathcal{D}$	$\mathcal{R}$	$\mathcal{R}$
Eve's state	D	A	H	H	V	A	V	D	A	V	A	H	V	A	V	D	H	V
Bob's basis	$\mathcal{R}$	$\mathcal{R}$	$\mathcal{D}$	$\mathcal{R}$	$\mathcal{D}$	$\mathcal{D}$	$\mathcal{D}$	$\mathcal{D}$	$\mathcal{R}$	$\mathcal{R}$	$\mathcal{R}$	$\mathcal{D}$	$\mathcal{R}$	$\mathcal{R}$	$\mathcal{R}$	$\mathcal{D}$	$\mathcal{R}$	$\mathcal{D}$
Bob's result	H	V	A	H	D	A	A	D	H	V	V	A	V	H	V	D	H	D
same basis	✓		✓	✓	✓			✓	✓			✓	✓		✓			
bits announced	0							0				1						
bits coincide	✓							✓				✗						

5.2.2 The Gap Between Theory and Implementation

In theory, the BB84 protocol has been rigorously proven secure [57] after a few incomplete attempts [52] [58] as mentioned by Brassard [59]. However, in reality much depends on the actual experimental implementation. The first experiment performed by Bennett, Brassard and three of their students was very noisy, and the apparatus made different sounds when generating a "0" or a "1" such that an eavesdropper could easily get the key by only listening to the experiment [59]. This particular problem has been solved in the meantime, but there are still lots of other difficulties. A severe one is that sending always

only one photon is complicated, and photon detectors do not have a high single photon detection efficiency. Usually, weak laser pulses with an average number of photons per pulse below 1 are used. Most of these pulses are then vacuum pulses as they contain no photon at all. Nevertheless, it is impossible to prevent pulses from containing more than one photon. This led to the development of the so-called photon-number splitting attack [60] [61] [62]. To regain the security even when using (weak) laser pulses and to improve the transmission rate and thus the maximal distance, the decoy-state scheme has been invented [63] [64]. However, there are still many possible attempts such as for example the time-shift attack [65] [66] [67], the trojan horse attack [68], or the detector blinding attack [69] [70] to manipulate or exploit vulnerabilities of the devices used in the implementation of the quantum key distribution protocol. Summaries of possible and performed attacks are also given in Refs. [71], [72], and [73]. But although often solutions to the security leaks for the published attacks are immediately presented by the groups themselves or by follow up work of other groups, the problem is still that in this way the implementations can only be protected against publicly known attacks [73].

Another idea of dealing with the threat of imperfect implementations is to treat the entire setup as a *black box* which may even be built by an untrusted third party or Eve herself, i.e., making the protocol independent of the functioning of the utilized devices [74] [75] [76] [77]. This is named device-independent quantum key distribution as Alice and Bob do not have to know how their devices work.

Unfortunately, device-independent quantum key distribution also has some serious problems such as, for example, the low secret key rate making it unsuited for large distances [73] [78], and the proposed Bell test has never been successfully realized [73]. Thus, no such device-independent quantum key distribution has been successfully performed. However, since most attacks against conventional quantum key distribution implementations are against the detectors, the measurement devices seem to be the most vulnerable devices. This led to the invention of measurement-device-independent quantum key distribution by Lo, Curty, and Qi [78], and independently by Braunstein and Pirandola [79], where only the measurement devices are considered as black boxes but the sources still have to be characterized. The characterization of the sources without information escaping to Eve is considered achievable [78].

In the measurement-device-independent setup, Alice and Bob send a part of their entangled states [79] [73] or one of the polarization states $|H\rangle$, $|V\rangle$, $|D\rangle$ or $|A\rangle$ [78] to an untrusted third party Charlie, or even Eve, who performs a Bell-state measurement, i.e., measures only the parity of Alice's and Bob's bits, and announces the outcomes publicly. Hence, Charlie and Eve cannot gain any information about the actual bits, and thus Charlie's detectors do not need to be protected against Eve [73]. By comparing a random subset of their obtained bits, Alice and Bob can test Charlie's honesty. For this kind of quantum key distribution, successful experiments have been reported both for time-bin encoded qubits [80] [81] and for polarization encoded qubits [82] [83].

Another possible advantage of measurement-device-independent quantum key distribution is that Charlie could operate as some kind of (untrusted) *server*, connecting many *clients* who would then only have to possess the sources but do not need to own the detection devices each [73].

In the following, we investigate a variation of measurement-device-independent implementations based on single-photon Bell state measurements (SBSM) [84] [85] [86], which is also called detector-device-independent quantum key distribution. The SBSM scheme

uses two degrees of freedom of a single photon such as the polarization and the phase, and therefore two qubits can be encoded using a single photon [84]. The advantage is that no interference of two photons coming from two different sources is needed, and thus the key rate increases compared to other measurement-device independent quantum key distribution implementations [84] [87]. For detector-device-independent quantum key distribution, the measurement devices are uncharacterized but all elements of the setup have to be known at least to Bob who performs the SBSM. So here the *black box* has a slightly different meaning: Bob has to know which optical elements are contained in the setup, but he does not need to know how they work in detail [85]. Otherwise, since Bob's laboratory has to be accessible to Alice's photons, Eve could send in her own pulses and if the SBSM was completely untrusted, this would provide an opportunity for attacks [88]. However, taking the necessary precautions against such attacks, detector-device independent quantum key distribution may be a compromise as it seems to be more viable than device-independent or measurement-device-independent quantum key distribution. Moreover, it is still secure against a large class of attacks.

In the following, we will show that we can simulate an experiment of this kind with the discrete-event simulation method which is non-quantum and strictly satisfies Einstein's criterion of locality. That means we can produce the same correlations as the Bell-state measurement without using Bell states. The implementation we consider in the next section uses path and time-bin encoding and a relative phase as degrees of freedom [87].

5.2.3 Discrete-Event Simulation of a Quantum Key Distribution Protocol

We specifically discuss the detector-device independent implementation of the quantum key distribution protocol based on a SBSM presented in Ref. [87]. The two qubits are encoded in two degrees of freedom of a photon, namely the phase and the path and time-bin in this case. The BB84 protocol [51] and Ekert's protocol [89] have been discussed in general by means of the discrete-event simulation in Ref. [11] using only the polarization degree of freedom of the photons such that one photon represents only one qubit. Moreover, the simulations differ in that the simulation method applied in Ref. [11] comes without a learning machine, but makes (partially) use of postselection.

First, we examine how the experiment works in theory, and then we simulate it by means of the discrete-event simulation method and compare the results. This type of experiment is interesting from the point of view of discrete-event simulations as the security of detector-device independent quantum key distribution relies on the input and output statistics of the measurement [85]. They are attributed to Bell states that exhibit entanglement in quantum theory, but we will produce the same correlations with a simulation where no Bell states appear.

Theoretical Description of the Experiment

The setup of the experiment is shown in Fig. 5.1. The protocol works in detail as follows: Alice chooses a phase $\alpha \in \{0, \pi/2, \pi, 3\pi/2\}$ and sends a photon into her interferometer. After entering Alice's unbalanced Mach-Zehnder interferometer through the first beam splitter at $t = 0$, the photon is in a superposition of taking the short path ($|s\rangle$) and the

long path ($|l\rangle$) such that its state $|\varphi_1\rangle$ is given by

$$|\varphi_1\rangle = \frac{1}{\sqrt{2}}\left(|s\rangle + i|l\rangle\right) \otimes |t = 0\rangle, \tag{5.15}$$

where we base our notation on the one used in [87]. The part in the long arm of the Mach-Zehnder interferometer then collects the phase shift α chosen by Alice. The photon takes the time t_s for the short arm of the interferometer and the time $t_s + t_d$ for the long arm where we choose w.l.o.g. the time delay t_d such that $e^{2\pi i f t_d} = 1$ (otherwise we would end up with a constant shift of α and β). So immediately before the second beam splitter, the state of the photon is given by

$$|\varphi_2\rangle = \frac{e^{2\pi i f t_s}}{\sqrt{2}}\left(|s\rangle|t_s\rangle + ie^{i\alpha}|l\rangle|t_s + t_d\rangle\right). \tag{5.16}$$

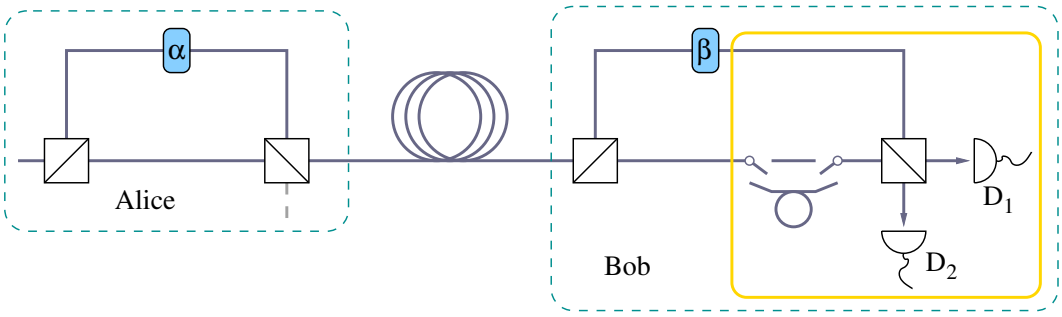

Figure 5.1: Setup of the experiment performing the SBSM quantum key distribution proposed in Ref. [87]. White boxes with a diagonal line represent beam splitters, blue plates with α and β denote phase shifters with phase shift α or β, respectively. Alice's and Bob's laboratories are marked by the cyan dashed boxes. The gray dashed line leaving Alice's second beam splitter denotes discarded photons leaving the setup. The yellow line encircles the part of Bob's apparatus which he can treat as a black box. Within this part, a switch which delays these photons that took the short arm in Alice's interferometer is contained. The half circles represent the detectors for the Bell-state measurement.

Due to the difference in the path and time-bin degree of freedom, there is no interference at Alice's second beam splitter and we get for the state after the beam splitter

$$|\varphi_3\rangle = \frac{e^{2\pi i f t_s}}{2}\Big(\big(|c\rangle + i|d\rangle\big)|t_s\rangle + ie^{i\alpha}\big(|d\rangle + i|c\rangle\big)|t_s + t_d\rangle\Big), \tag{5.17}$$

where $|c\rangle$ and $|d\rangle$ denote the output states of the beam splitter transformation

$$T_{A_2} = \frac{1}{\sqrt{2}}\big(|c\rangle + i|d\rangle\big)\langle s| + \frac{1}{\sqrt{2}}\big(i|c\rangle + |d\rangle\big)\langle l|. \tag{5.18}$$

The state $|c\rangle$ corresponds to the output which is still used, and $|d\rangle$ denotes the state leaving at the output which is discarded. As we consider in the following only photons in the state $|c\rangle$, the state describing the photons which leave Alice's laboratory is given by

$$|\varphi_4\rangle = \frac{e^{2\pi i f t_s}}{2}|c\rangle\left(|t_s\rangle - e^{i\alpha}|t_s + t_d\rangle\right). \tag{5.19}$$

The photon leaves Alice's laboratory and travels to Bob's laboratory which takes a time t_t and therefore adds a global phase to the state. At Bob's first beam splitter, the photon's state is transformed by

$$T_{B_1} = \frac{1}{\sqrt{2}}\big(|S\rangle + i|L\rangle\big)\langle c| + \frac{1}{\sqrt{2}}\big(i|S\rangle + |L\rangle\big)\langle e|, \tag{5.20}$$

where $|e\rangle$ denotes the empty input of the beam splitter, $|S\rangle$ represents the short path, and $|L\rangle$ denotes the long path of Bob's interferometer. The resulting state is given by

$$|\varphi_5\rangle = \frac{e^{2\pi i f(t_s+t_t)}}{2\sqrt{2}}\Big(\left(|S\rangle + i|L\rangle\right)|t_s + t_t\rangle - e^{i\alpha}\left(|S\rangle + i|L\rangle\right)|t_s + t_d + t_t\rangle\Big). \tag{5.21}$$

Bob chooses his phase shift $\beta \in \{0,\, \pi/2,\, \pi,\, 3\pi/2\}$ for the long arm of the interferometer. There is a switch in the short arm of the interferometer which delays only those photons arriving at time $t_s + t_t$ by a time $2t_d$. So the state we have at Bob's second beam splitter is represented by

$$|\varphi_6\rangle = \frac{e^{2\pi i f(2t_s+t_t)}}{2\sqrt{2}}\Big(|S\rangle|t_1\rangle + ie^{i\beta}|L\rangle|t_0\rangle - e^{i\alpha}|S\rangle|t_0\rangle - ie^{i(\alpha+\beta)}|L\rangle|t_1\rangle\Big) \tag{5.22}$$

$$= \frac{e^{2\pi i f(2t_s+t_t)}}{2\sqrt{2}}\Big(\left(|S\rangle - ie^{i(\alpha+\beta)}|L\rangle\right)|t_1\rangle + \left(ie^{i\beta}|L\rangle - e^{i\alpha}|S\rangle\right)|t_0\rangle\Big), \tag{5.23}$$

where $t_0 = 2t_s + t_d + t_t$ and $t_1 = 2t_s + 2t_d + t_t$. Finally, the photons have to pass the last beam splitter, whose transformation is given by

$$T_{B_2} = \frac{1}{\sqrt{2}}\big(|1\rangle + i|2\rangle\big)\langle S| + \frac{1}{\sqrt{2}}\big(i|1\rangle + |2\rangle\big)\langle L|, \tag{5.24}$$

where $|1\rangle$ denotes the path to detector D_1, and $|2\rangle$ denotes the path to detector D_2. The state of the photons is then given by

$$|\varphi_7\rangle = \frac{e^{2\pi i f(2t_s+t_t)}}{4}\Big(\left(|1\rangle + i|2\rangle\right)|t_1\rangle - ie^{i(\alpha+\beta)}\left(|2\rangle + i|1\rangle\right)|t_1\rangle + ie^{i\beta}\left(|2\rangle + i|1\rangle\right)|t_0\rangle - e^{i\alpha}\left(|1\rangle + i|2\rangle\right)|t_0\rangle\Big) \tag{5.25}$$

$$= \frac{e^{2\pi i f(2t_s+t_t)}}{4}\Big(\left(1 + e^{i(\alpha+\beta)}\right)|1\rangle|t_1\rangle + i\left(1 - e^{i(\alpha+\beta)}\right)|2\rangle|t_1\rangle - \left(e^{i\alpha} + e^{i\beta}\right)|1\rangle|t_0\rangle - i\left(e^{i\alpha} - e^{i\beta}\right)|2\rangle|t_0\rangle\Big). \tag{5.26}$$

Bob can now measure one of the four cases

- detector 1 clicks at time t_0 with probability $P(D_1, t_0) = (1 + \cos(\alpha - \beta))/8$ (5.27)
- detector 2 clicks at time t_0 with probability $P(D_2, t_0) = (1 - \cos(\alpha - \beta))/8$ (5.28)
- detector 1 clicks at time t_1 with probability $P(D_1, t_1) = (1 + \cos(\alpha + \beta))/8$ (5.29)
- detector 2 clicks at time t_1 with probability $P(D_2, t_1) = (1 - \cos(\alpha + \beta))/8.$ (5.30)

With probability $1/2$, the photon was already discarded in Alice's laboratory. The cases to measure the photon at time t_0 or at time t_1 are equally likely and independent of the phase

shifts α and β as $P(t_0) = P(D_1, t_0) + P(D_2, t_0) = 1/4 = P(D_1, t_1) + P(D_2, t_1) = P(t_1)$. So whether a detector clicks at time t_0 or at time t_1 cannot be controlled by Alice and Bob. The phase shifts α and β determine whether the two states which take a time t_0, namely the photon took the long arm and then the short arm ($|lS\rangle$) or vice versa ($|sL\rangle$), interfere constructively at detector 1 and destructively at detector 2 ($\alpha = \beta$) or vice versa ($|\alpha - \beta| = \pi$). A similar rule, but with different dependence on α and β, applies for states which take a time t_1, namely the photon taking twice the long arm ($|lL\rangle$) or twice the short arm with the extra delay ($|sS\rangle$). A detector click at time t_0 or time t_1 indicates whether the state collapsed to a state where $|lS\rangle$ and $|sL\rangle$ interfere or to a state where $|lL\rangle$ and $|sS\rangle$ interfere. The number of the detector that clicks gives information about the relative phase such that the four possible combinations of detector numbers and detection times can be assigned to a measurement of the four states

$$|\Phi^+\rangle = \frac{|sS\rangle + |lL\rangle}{\sqrt{2}} \tag{5.31}$$

$$|\Phi^-\rangle = \frac{|sS\rangle - |lL\rangle}{\sqrt{2}} \tag{5.32}$$

$$|\Psi^+\rangle = \frac{|lS\rangle + |sL\rangle}{\sqrt{2}} \tag{5.33}$$

$$|\Psi^-\rangle = \frac{|lS\rangle - |sL\rangle}{\sqrt{2}}, \tag{5.34}$$

which are the maximally entangled states, also called Bell states, for the state

$$|\psi\rangle = \frac{1}{2}\left(|sS\rangle + e^{i(\alpha+\beta)}|lL\rangle + e^{i\alpha}|lS\rangle + e^{i\beta}|sL\rangle\right). \tag{5.35}$$

The correspondence can be made since the probabilities to measure a state $|\Phi^\pm\rangle$ or $|\Psi^\pm\rangle$ are

$$P(\Phi^+ \,|\, \alpha, \beta) = \big|\big||\Phi^+\rangle\langle\Phi^+|\psi\rangle\big|\big|^2 = \frac{1 + \cos(\alpha + \beta)}{4} \tag{5.36}$$

$$P(\Phi^- \,|\, \alpha, \beta) = \big|\big||\Phi^-\rangle\langle\Phi^-|\psi\rangle\big|\big|^2 = \frac{1 - \cos(\alpha + \beta)}{4} \tag{5.37}$$

$$P(\Psi^+ \,|\, \alpha, \beta) = \big|\big||\Psi^+\rangle\langle\Psi^+|\psi\rangle\big|\big|^2 = \frac{1 + \cos(\alpha - \beta)}{4} \tag{5.38}$$

$$P(\Psi^- \,|\, \alpha, \beta) = \big|\big||\Psi^-\rangle\langle\Psi^-|\psi\rangle\big|\big|^2 = \frac{1 - \cos(\alpha - \beta)}{4}, \tag{5.39}$$

which have the same dependence on α and β as the four possible measurement outcomes of Bob (Eqs. (5.27) - (5.30)). The only difference is the factor one half because $|\varphi\rangle$ is not normalized due to the rejection of the photon with probability 1/2 after the second beam splitter in Alice's laboratory. The correspondence between the measurement outcome and the Bell states is given in Table 5.3.

Since Alice and Bob can manipulate the relative phases of $|lS\rangle$ and $|sL\rangle$, and of $|sS\rangle$ and $|lL\rangle$ by choosing their phase shifts α and β, they can affect the probabilities of the measurement outcomes. This can be exploited such that Bob can determine Alice's phase shift α through his choice of β if α and β are either both chosen from the set $\mathcal{I} := \{0, \pi\}$ or both chosen from the set $\mathcal{B} := \{\pi/2, 3\pi/2\}$. For example, say Bob chooses $\beta = \pi/2$.

If Alice also chooses $\alpha = \pi/2$, the probabilities for the detector clicks are then

$$P(D_1, t_0|\alpha = \beta = \pi/2) = P(D_2, t_1|\alpha = \beta = \pi/2) = 1/4 \tag{5.40}$$

$$\text{and} \quad P(D_2, t_0|\alpha = \beta = \pi/2) = P(D_1, t_1|\alpha = \beta = \pi/2) = 0 \tag{5.41}$$

or if Alice chooses $\alpha = 3\pi/2$,

$$P(D_1, t_0|\alpha = 3\pi/2, \beta = \pi/2) = P(D_2, t_1|\alpha = 3\pi/2, \beta = \pi/2) = 0 \tag{5.42}$$

$$\text{and} \quad P(D_2, t_0|\alpha = 3\pi/2, \beta = \pi/2) = P(D_1, t_1|\alpha = 3\pi/2, \beta = \pi/2) = 1/4. \tag{5.43}$$

However, if Alice chooses $\alpha = 0$ or $\alpha = \pi$, the probabilities for the different detection times and detector numbers are all the same:

$$P(D_1, t_0|\alpha = 0, \beta = \pi/2) = P(D_1, t_1|\alpha = 0, \beta = \pi/2) = 1/8 \tag{5.44}$$

$$P(D_2, t_0|\alpha = 0, \beta = \pi/2) = P(D_2, t_1|\alpha = 0, \beta = \pi/2) = 1/8 \tag{5.45}$$

$$P(D_1, t_0|\alpha = \pi, \beta = \pi/2) = P(D_1, t_1|\alpha = \pi, \beta = \pi/2) = 1/8 \tag{5.46}$$

$$P(D_2, t_0|\alpha = \pi, \beta = \pi/2) = P(D_2, t_1|\alpha = \pi, \beta = \pi/2) = 1/8. \tag{5.47}$$

If Bob measures the detector click at time t_0 from detector D_1 and he assumes that Alice also chose α from the set $\mathcal{B}$, he estimates that $\alpha = \pi/2$.

Table 5.3: Relation between detection time and detector number and the corresponding Bell state. The detection time determines whether the state collapses to $|\Psi^{\pm}\rangle$ or $|\Phi^{\pm}\rangle$. This outcome is random. Which detector clicks is predetermined by the relative phase of the two interfering states. Detector D_1 clicks if the relative phase is zero, and detector D_2 clicks if the relative phase is π.

Time	Detector	Bell state
t_0	D_1	$\|\Psi^+\rangle$
	D_2	$\|\Psi^-\rangle$
t_1	D_1	$\|\Phi^+\rangle$
	D_2	$\|\Phi^-\rangle$

Table 5.4 shows the possible measurement outcomes for all combinations of possible values for α and β. All combinations where α and β are chosen from the same set lead to an unambiguous relation between the detection time and detector number and the phase shift α. In the cases where Alice and Bob choose α and β from different sets, Bob's estimate based on the assumption that the phase shifts are chosen from the same set is correct only with probability 1/2, so these cases have to be discarded as the measurement outcome is uncorrelated with the phases α and β.

For this purpose, in the next step Alice and Bob have to communicate over an authenticated, classical channel whether they chose the phase shifts α and β from the set $\mathcal{I}$ or $\mathcal{B}$. In those cases where they chose α and β from the same set, Bob can determine Alice's phase shift α.

Using, for example, the convention that $\alpha = 0$ or $\alpha = \pi/2$ denote the bit "0", and that $\alpha = \pi$ or $\alpha = 3\pi/2$ denote the bit "1", Alice and Bob can distill a shared secret key as Bob is able to reconstruct Alice's initial bit. Which bit he has to choose depending on the measurement outcome and his phase shift β is shown in Table 5.5.

Table 5.4: Possible detection outcomes of the Bell-state measurement depending on the phase shifts α and β chosen by Alice and Bob, respectively. The possible results in a field are equally likely. This table is also given in Ref. [87].

$\alpha \backslash \beta$	0	π	$\pi/2$	$3\pi/2$
0	D_1 at $t_0 : \lvert\Psi^+\rangle$ D_1 at $t_1 : \lvert\Phi^+\rangle$	D_2 at $t_0 : \lvert\Psi^-\rangle$ D_2 at $t_1 : \lvert\Phi^-\rangle$	all possible	all possible
π	D_2 at $t_0 : \lvert\Psi^-\rangle$ D_2 at $t_1 : \lvert\Phi^-\rangle$	D_1 at $t_0 : \lvert\Psi^+\rangle$ D_1 at $t_1 : \lvert\Phi^+\rangle$	all possible	all possible
$\pi/2$	all possible	all possible	D_1 at $t_0 : \lvert\Psi^+\rangle$ D_2 at $t_1 : \lvert\Phi^-\rangle$	D_2 at $t_0 : \lvert\Psi^-\rangle$ D_1 at $t_1 : \lvert\Phi^+\rangle$
$3\pi/2$	all possible	all possible	D_2 at $t_0 : \lvert\Psi^-\rangle$ D_1 at $t_1 : \lvert\Phi^+\rangle$	D_1 at $t_0 : \lvert\Psi^+\rangle$ D_2 at $t_1 : \lvert\Phi^-\rangle$

Table 5.5: Detector number and detection time to bit conversion. Depending on the detector number, detection time, and the phase shift β, Alice's initial bit can be guessed by Bob according to this table. If α and β are from the same set, the bit distilled by Bob coincides with Alice's bit.

Detector number and time	Bob's phase β	Bit distilled by Bob
D_1 at t_0	0 or $\pi/2$	0
	π or $3\pi/2$	1
D_2 at t_0	0 or $\pi/2$	1
	π or $3\pi/2$	0
D_1 at t_1	0 or $3\pi/2$	0
	π or $\pi/2$	1
D_2 at t_1	0 or $3\pi/2$	1
	π or $\pi/2$	0

In the following, we will discuss the discrete-event simulation of this protocol and see how we have to use the time to achieve the desired results.

The Simulation

Before we start with the complete protocol discussed in the previous section, we have a look at the normalized detector counts depending on the phase shifts α and β. In order to do this, we scan β from 0° to 360° in steps of 5° for $\alpha = 0°$, $\alpha = 45°$, $\alpha = 90°$, and $\alpha = 135°$. This will serve as a check whether the simulation reproduces the same dependence as the Bell-state measurement.

For the discrete-event simulation of the experiment introduced in the previous section, we used a source with fluctuating frequency, i.e., the photons get a frequency $f + \nu$ where f is fixed and ν is a random number distributed as described by Eq. (2.2) in section 2.3. The parameters of the source are chosen to be $f = 193414\,\mathrm{GHz}$ such that $c/\lambda \approx f$, where c is the speed of light and $\lambda = 1550\,\mathrm{nm}$ as used in the experiment [87], and $\sigma = 5\,\mathrm{GHz}$. We have to use the frequency fluctuating source here as time is relevant in the experiment but only the phase is stored in the message. To avoid that we end up with only a fixed phase shift $e^{2\pi i f t_d}$, where t_d is the time delay a photon accumulates due to the difference in the

path lengths between the short arm and the long arm, we have to vary the frequency f slightly such that the time delay really causes decoherence at the beam splitters which are linear elements. We can then use the simple beam splitter without learning machine. The time delay is chosen to be $t_d = 1\,\text{ns}$. For the switch, we can use an ideal one which adds a time delay $2t_d$ only to those photons that took the short arm in Alice's interferometer. This is not a problem in the simulation, as we can add a time tag to the photon in addition to the message, telling us at the switch whether the delay has to be added or not. The phase shifts of α and β are implemented as described in section 2.4.

At the detectors, the photons arrive either at time t_0 or at time t_1, so photons that arrive at the same time can interfere here, also for the fluctuating source as detectors are nonlinear elements, and thus the detection of photons depends on previous ones even with different frequencies [90]. Therefore, we have to use the advanced detectors introduced in section 2.6 which are capable of producing interference effects. As we need four different interference patterns (two at time t_0 and two at time t_1) but we have only two detectors, we have to make the detectors able to store two patterns. This means that a detector has to store four complex numbers for the learning machine, namely $Y_v^{t_0}$, $Y_h^{t_0}$, $Y_v^{t_1}$, and $Y_h^{t_1}$, such that the time degree of freedom is explicitly taken into account. The parameters of the detectors were chosen to be $\gamma = 0.98$ and $\eta = 0.153$ as in the experiment. A test of the effective efficiency of the simulated detectors resulted in $\eta_{eff} = 0.1524$.

For each setting of α and β, $N = 1\,000\,000$ events are generated where the polarization and the initial phase are random but fixed for each setting. The source emits $N_\nu = 200$ photons with a constant fluctuation ν of the frequency until a new random ν is generated. The photons are sent through the setup which is visualized in Fig. 5.1. Photons leaving the second beam splitter through output port 1 are discarded. Those photons arriving at one of the detectors affect the internal state of the learning machine and may produce a click. For plotting, the detector counts N_i, $i \in \{(D_1, t_0), (D_1, t_1), (D_2, t_0), (D_2, t_1)\}$, are normalized by the sum of all detector counts $\sum_i N_i$ instead of the total number of events N.

The results regarding the dependence of the normalized detector counts on the phase shifts α and β are shown in Fig. 5.2. The relations between the detectors' clicks are the same for $\alpha = 0$ (Fig. 5.2a) and $\alpha = \pi$ (Fig. 5.2c) but shifted by π, and for $\alpha = \pi/2$ (Fig. 5.2b) and $\alpha = 3\pi/2$ (Fig. 5.2d) also shifted by π. This corresponds to the upper left and lower right blocks in Table 5.4. The results coincide with the experimental data given in Ref. [84], where the same plots are made for a slightly different protocol which utilizes the polarization instead of the time for the second degree of freedom. However, we obtain the same relations between the four detection outcomes which also agree with the results from the previous section where we discussed the protocol analytically. So we have verified that our simulation gives the same results for the dependence on the phase shifts α and β as the experiment and the theory.

Now that we have seen that the measurement in the simulation works as it should, we can investigate the part of the protocol which deals with the distribution of the secret key. If we want a secret key length of about $M/2$ bits, we have to generate M random settings for the phase shifts α and β because in about one half of the random settings, α and β are not from the same set $\mathcal{I}$ or $\mathcal{B}$, and Alice's bit cannot be determined with certainty. As the phase shifts α and β should be chosen at random in this part of the simulation, we select two uniformly distributed random numbers $R_1, R_2 \in \{0, 1, 2, 3\}$ such that $\alpha = R_1 \cdot \pi/2$, and $\beta = R_2 \cdot \pi/2$. For each setting of α and β, we generate n events

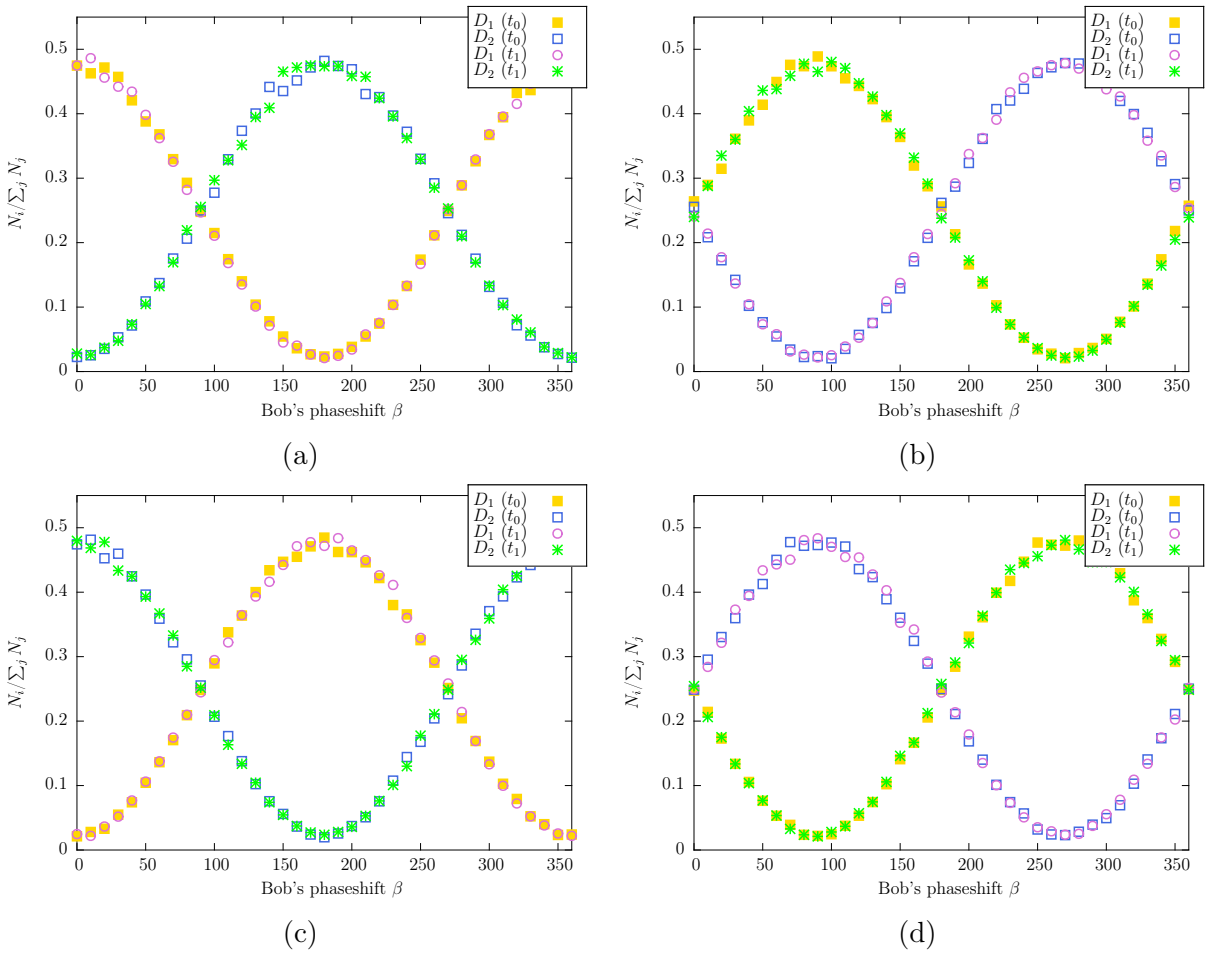

Figure 5.2: Results for the normalized detector counts $N_i/\sum_j N_j$ depending on the phase shift β chosen by Bob for Alice's phase shift α being (a) $\alpha = 0$ (b) $\alpha = \pi/2$ (c) $\alpha = \pi$ (d) $\alpha = 3\pi/2$. If Alice and Bob choose their phase shifts from the same set $\mathcal{I} = \{0, \pi\}$ or $\mathcal{B} = \{\pi/2, 3\pi/2\}$, Bob can determine Alice's choice as in these cases his outcome is unambiguous. For each setting of α and β, the number of generated events was $N = 1\,000\,000$.

such that we have a total number of $M \cdot n$ events with M blocks of n successive events with the same settings for α and β. This is necessary as with the learning machine of the detectors we can achieve the correct results on average, but we need a certain number of events to train the learning machine.

The transmissions and measurement work as discussed in the previous part, but now the detector number and detection time have to be converted into "0" or "1" depending on the phase shift β. The conversion is done according to Table 5.5 for each detected event. In each of the M blocks with fixed settings for α and β, a `bit_counter` is increased by one whenever a measurement outcome and phase setting of Bob indicate that Alice's bit is 1. Divided by all detected events in this block, Bob achieves an average bit between 0 and 1. In the cases where the bit can be determined with certainty, i.e., α and β are in the same set $\mathcal{I}$ or $\mathcal{B}$, the average bit should be close to 0 or 1. Otherwise, the average bit is around 0.5. Still, the average bit has to be rounded to 0 or 1, as in the original protocol Bob can only get the outcome 0 or 1. The next step in the protocol is that

Alice and Bob communicate the sets $\mathcal{I}$ and $\mathcal{B}$ of their chosen phases α and β, so we check whether $|R_1 - R_2| \bmod 2 = 0$. If the random numbers R_1 and R_2 satisfy this condition, the bit is included in the key, otherwise the bit is discarded. Additionally, we also check whether the bit distilled by Bob in this procedure coincides with the bit Alice started with. Excerpts of the results for $n = 1000$ and $n = 5000$ are given in Table 5.6 and Table 5.7, respectively.

Table 5.6: Summarized protocol and results including the secret key for $n = 1000$. From $M = 100$ generated settings, only an excerpt of 20 settings is shown, including from left to right: the initial bit of Alice, the phase shifts α of Alice, and β of Bob, the average bit and rounded bit distilled by Bob, the outcome of the test whether α and β are from the same set, and if yes, the check of the correctness of the distilled bit, and finally the bit used for the key. All bits that could be determined with certainty from the theoretical point of view are correctly determined in this excerpt. There is one bit flip error in the key generated from the 100 settings (not shown in this excerpt). Nevertheless, even in this excerpt some average bits are close to 0.5 although Bob should be able to determine Alice's bit with certainty. The key gained from this excerpt is 15 bits long: 010011100101110

Alice's bit	α	β	average bit	rounded bit	same set	correct	key
1	$3\pi/2$	0	0.612676	1	no		
0	$\pi/2$	π	0.406504	0	no		
0	0	0	0.280822	0	yes	yes	0
1	$3\pi/2$	$\pi/2$	0.663866	1	yes	yes	1
0	0	0	0.347458	0	yes	yes	0
0	0	0	0.362903	0	yes	yes	0
1	$3\pi/2$	π	0.609091	1	no		
1	π	π	0.723077	1	yes	yes	1
1	$3\pi/2$	$\pi/2$	0.54023	1	yes	yes	1
1	π	π	0.734694	1	yes	yes	1
0	$\pi/2$	$3\pi/2$	0.415842	0	yes	yes	0
0	$\pi/2$	$3\pi/2$	0.411215	0	yes	yes	0
1	π	π	0.680272	1	yes	yes	1
0	$\pi/2$	$\pi/2$	0.424528	0	yes	yes	0
0	$\pi/2$	0	0.423529	0	no		
1	π	π	0.545455	1	yes	yes	1
1	π	π	0.538462	1	yes	yes	1
1	$3\pi/2$	$3\pi/2$	0.614583	1	yes	yes	1
0	0	$\pi/2$	0.46875	0	no		
0	$\pi/2$	$3\pi/2$	0.395833	0	yes	yes	0

For increasing n, we can achieve better results in the sense that the average bits become more precise: for $n = 5000$ the average bits always tend clearly to the correct bit while for $n = 1000$ the correct bit does not always emerge clearly from the averaged bit. In the data corresponding to the excerpt in Table 5.6, this resulted in one error per $M = 100$ settings. Nevertheless, the results are all correctly rounded for $n \geq 2000$ (results for $n = 2000$ not shown). So we need n to be in the order of 10^3 events to get the correct, averaged results per setting. One may say that this is not a satisfying result; however, in the real experiment better key generation rates were not achieved either [87]. Only in

the extrapolation to a transmission distance of 0 km, the key generation rate approaches approximately 6×10^{-2}/ pulse.

Table 5.7: Summarized protocol and results including the secret key for $n = 5000$. From $M = 100$ generated settings, only an excerpt of 20 settings is shown. The same quantities as in Table 5.6 are given. All bits that could be determined with certainty from the theoretical point of view are correctly determined in this excerpt as well as in the whole dataset. For $n = 5000$, the results are more clearly than for $n = 1000$. The key gained from this excerpt is 11 bits long: 00010110011

Alice's bit	α	β	average bit	rounded bit	same set	correct	key
1	$3\pi/2$	0	0.56213	1	no		
0	0	π	0.236111	0	yes	yes	0
1	$3\pi/2$	0	0.506383	1	no		
0	0	0	0.14881	0	yes	yes	0
0	$\pi/2$	$3\pi/2$	0.129032	0	yes	yes	0
1	$3\pi/2$	$\pi/2$	0.800676	1	yes	yes	1
1	π	$\pi/2$	0.512987	1	no		
0	0	0	0.144118	0	yes	yes	0
1	π	$\pi/2$	0.508021	1	no		
1	π	$\pi/2$	0.464072	0	no		
1	π	0	0.831776	1	yes	yes	1
1	$3\pi/2$	$\pi/2$	0.845426	1	yes	yes	1
0	$\pi/2$	$\pi/2$	0.117834	0	yes	yes	0
1	π	$3\pi/2$	0.513158	1	no		
1	$3\pi/2$	π	0.482759	0	no		
0	0	π	0.166667	0	yes	yes	0
1	π	0	0.85489	1	yes	yes	1
0	0	$\pi/2$	0.452107	0	no		
1	$3\pi/2$	0	0.530675	1	no		
1	π	π	0.792	1	yes	yes	1

Conclusion

We have demonstrated that it is possible to simulate a quantum key distribution protocol with a discrete-event simulation. The simulated protocol is a detector-device independent version of the BB84 protocol employing a Bell-state measurement. The important fact about this demonstration is that the discrete-event simulation is capable of reproducing the correlations attributed to Bell states, which are the maximally entangled states, within quantum theory. But the discrete-event simulation makes no use of quantum theory, not to mention entanglement. With the discrete-event simulation, we are able to achieve a key rate of $\approx 10^{-3}$/ event which lies in the range of key rates achievable in the experiment (10^{-2} to 10^{-7}/ pulse). Although the discrete-event simulation method strictly satisfies Einstein's criterion of locality, we can obtain the same correlations that are attributed to Bell states within quantum theory.

6 Franson-Interferometer

In 1989, Franson proposed an experimental setup consisting of two unbalanced Mach-Zehnder interferometers to measure the fourth-order interference between photon-pairs emitted by an atom [91]. The atom is supposed to have three energy levels $E_3 > E_2 > E_1$ such that the exited state with energy E_3 is metastable with a relatively long lifetime T_l, the state with energy E_2 is unstable with a very short lifetime T_s, and the state with energy E_1 is either the ground state or a stable state with a very long lifetime. Hence, when an excited atom emits a photon with energy $E_3 - E_2$, it almost immediately emits a second photon with energy $E_2 - E_1$. Due to the short lifetime T_s, the uncertainty in the frequencies of both photons $\sigma_\nu \sim {}^1/_{T_s}$ is large compared to the uncertainty in the sum of the frequencies $\Delta f \sim {}^1/_{T_l}$ [91]. Choosing the time delay ΔT in the unbalanced Mach-Zehnder interferometer such that $T_l \gg \Delta T \gg T_s$, the cases of early emitted photons taking both the long paths in the interferometers and of late emitted photons taking both the short paths in the interferometers become indistinguishable such that the corresponding probability amplitudes can interfere [91]. For that reason, photon pairs exhibiting this feature are called energy-time entangled within quantum theory. Additionally, choosing $\Delta T \gg T_s$ allows for identification of the cases where one of the photons takes the long path and the other one the short path. They can then be removed via postselection by setting the coincidence window $\tau \ll \Delta T$ since the photons taking two paths of different lengths also differ in the arrival time by approximately $\Delta T \pm T_s \approx \Delta T \gg \tau$.

After Franson's proposal, experiments with the aim of measuring the fourth-order interferences have been performed where the photon-pairs usually originate from down-conversion in nonlinear crystals. The first experiments successfully measuring the fourth-order interferences still attained visibilities $\mathcal{V}$ below $\mathcal{V} = 0.5$ [92] [93] [94], but later also visibilities exceeding $\mathcal{V} = 0.5$ were measured [95]. More recent experiments based on the Franson-interferometer are often related to quantum key distribution [96] [97] [98].

We aim at obtaining the fourth-order interference of this kind of experiment by means of a discrete-event simulation as energy-time entangled systems have not yet been examined in this framework. But before we start with the simulation, we investigate the theoretical outcomes of classical wave theory and quantum mechanics to have qualitative results to compare with.

6.1 Classical and Quantum Theoretical Correlations

The setup of the Franson-interferometer is shown in Fig. 6.1. A source emits pairs of photons with frequencies f^+ and f^- within a small time window, where the sum of the frequencies $f^+ + f^-$ has a very small uncertainty compared to the frequencies f^+ and f^- themselves. Inspired by Ref. [99], we will assume in the calculation that $f^+ = f_0 + \nu$ and

$f^- = f_0 - \nu$ where ν is a random number taken from the distribution

$$p(\nu) = \frac{1}{\sqrt{2\pi}\sigma} e^{-\nu^2/(2\sigma^2)}, \tag{6.1}$$

with σ being the uncertainty in the frequencies f^+ and f^-. As the uncertainty in f^+ and f^- is quite large, we do not expect to see any single-photon interference.

After the generation, the photons travel in opposite directions towards the unbalanced Mach-Zehnder interferometers, which contain phase shifters that add a phase φ_A or φ_B, respectively. The detectors on the right are labeled by D_{A+} and D_{A-}, and the detectors on the left are labeled by D_{B+} and D_{B-}. In the calculations of averages, the detectors labeled with a minus sign will count as -1 detection events and detectors labeled with a plus sign will count as $+1$ detection events.

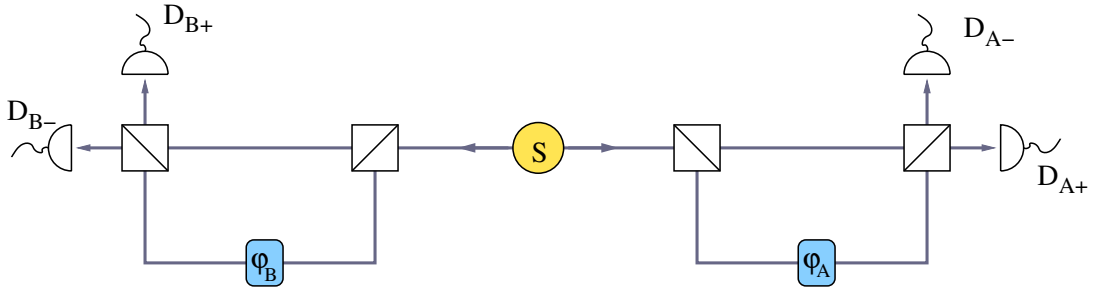

Figure 6.1: Setup of the Franson-Interferometer experiment. The circle with the S denotes the two-photon source emitting two photons of varying frequencies f^+ and f^- such that $f^+ + f^- = 2f_0$ which is fixed. The white boxes with a diagonal line represent beam splitters. Blue boxes with label φ_A or φ_B are phase shifters with phase shift φ_A or φ_B, respectively. Half circles with a wiggly line denote photon detectors and are labeled by D_{B+}, D_{B-}, D_{A+}, and D_{A-}.

6.1.1 Classical Description

Using the classical approach, for simplicity with plain waves, we have to add the amplitudes corresponding to the possible paths at the level of the detectors. Beginning with the same initial amplitude $A_0 > 0$ but different phases ψ_A and ψ_B for the right and left traveling waves, respectively, we get the amplitudes A_+ and A_- (B_+ and B_-) at the detectors D_{A+} and D_{A-} (D_{B+} and D_{B-}):

$$A_+ = A_0 e^{i\psi_A}\left(e^{2\pi i f^- t_0} - e^{2\pi i f^-(t_0+\Delta T)+i\varphi_A}\right) = A_0 e^{i\psi_A+2\pi i f^- t_0}\left(1 - e^{2\pi i f^-\Delta T+i\varphi_A}\right) \tag{6.2}$$

$$A_- = A_0 e^{i\psi_A}\left(ie^{2\pi i f^- t_0} + ie^{2\pi i f^-(t_0+\Delta T)+i\varphi_A}\right) = A_0 i e^{i\psi_A+2\pi i f^- t_0}\left(1 + e^{2\pi i f^-\Delta T+i\varphi_A}\right) \tag{6.3}$$

$$B_+ = A_0 e^{i\psi_B}\left(ie^{2\pi i f^+ t_0} + ie^{2\pi i f^+(t_0+\Delta T)+i\varphi_B}\right) = A_0 i e^{i\psi_B+2\pi i f^+ t_0}\left(1 + e^{2\pi i f^+\Delta T+i\varphi_B}\right) \tag{6.4}$$

$$B_- = A_0 e^{i\psi_B}\left(e^{2\pi i f^+ t_0} - e^{2\pi i f^+(t_0+\Delta T)+i\varphi_B}\right) = A_0 e^{i\psi_B+2\pi i f^+ t_0}\left(1 - e^{2\pi i f^+\Delta T+i\varphi_B}\right). \tag{6.5}$$

The intensities are computed from the modulus squared of the amplitudes given in Eqs. (6.2) - (6.5). For obtaining the correlation between two detectors, we have to multiply

the intensities of these two detectors, which gives for all possible combinations:

$$\begin{aligned}
I_{++} &= |A_+|^2|B_+|^2 = 4A_0^4\left(1-\cos\left(2\pi f^-\Delta T+\varphi_A\right)\right)\left(1+\cos\left(2\pi f^+\Delta T+\varphi_B\right)\right)\\
&= 2A_0^4\left(2-2\cos\left(2\pi f^-\Delta T+\varphi_A\right)+2\cos\left(2\pi f^+\Delta T+\varphi_B\right)\right.\\
&\quad \left.-\cos\left(-4\pi\nu\Delta T+\varphi_A-\varphi_B\right)-\cos\left(\varphi_0+\varphi_A+\varphi_B\right)\right) \qquad (6.6)\\
I_{--} &= |A_-|^2|B_-|^2 = 4A_0^4\left(1+\cos\left(2\pi f^-\Delta T+\varphi_A\right)\right)\left(1-\cos\left(2\pi f^+\Delta T+\varphi_B\right)\right)\\
&= 2A_0^4\left(2+2\cos\left(2\pi f^-\Delta T+\varphi_A\right)-2\cos\left(2\pi f^+\Delta T+\varphi_B\right)\right.\\
&\quad \left.-\cos\left(-4\pi\nu\Delta T+\varphi_A-\varphi_B\right)-\cos\left(\varphi_0+\varphi_A+\varphi_B\right)\right) \qquad (6.7)\\
I_{+-} &= |A_+|^2|B_-|^2 = 4A_0^4\left(1-\cos\left(2\pi f^-\Delta T+\varphi_A\right)\right)\left(1-\cos\left(2\pi f^+\Delta T+\varphi_B\right)\right)\\
&= 2A_0^4\left(2-2\cos\left(2\pi f^-\Delta T+\varphi_A\right)-2\cos\left(2\pi f^+\Delta T+\varphi_B\right)\right.\\
&\quad \left.+\cos\left(-4\pi\nu\Delta T+\varphi_A-\varphi_B\right)+\cos\left(\varphi_0+\varphi_A+\varphi_B\right)\right) \qquad (6.8)\\
I_{-+} &= |A_-|^2|B_+|^2 = 4A_0^4\left(1+\cos\left(2\pi f^-\Delta T+\varphi_A\right)\right)\left(1+\cos\left(2\pi f^+\Delta T+\varphi_B\right)\right)\\
&= 2A_0^4\left(2+2\cos\left(2\pi f^-\Delta T+\varphi_A\right)+2\cos\left(2\pi f^+\Delta T+\varphi_B\right)\right.\\
&\quad \left.+\cos\left(-4\pi\nu\Delta T+\varphi_A-\varphi_B\right)+\cos\left(\varphi_0+\varphi_A+\varphi_B\right)\right), \qquad (6.9)
\end{aligned}$$

where we defined $\varphi_0 = 4\pi f_0\Delta T$. In order to get the averaged correlations over the fluctuating frequencies, we have to integrate over all ν. Making use of the relation

$$\int_{-\infty}^{\infty}\frac{1}{\sqrt{2\pi}\sigma}e^{-\frac{x^2}{2\sigma^2}}\cos\left(2\pi xt+\theta\right)\,\mathrm{d}x = e^{-2\pi^2\sigma^2t^2}\cos\theta, \qquad (6.10)$$

we obtain for the averages of the correlations

$$\begin{aligned}
\langle I_{++}\rangle &= \int_{-\infty}^{\infty}p(\nu)I_{++}\,\mathrm{d}\nu\\
&= 2A_0^4\left(2-2e^{-2\pi^2\sigma^2\Delta T^2}\cos\left(\frac{\varphi_0}{2}+\varphi_A\right)+2e^{-2\pi^2\sigma^2\Delta T^2}\cos\left(\frac{\varphi_0}{2}+\varphi_B\right)\right.\\
&\quad \left.-e^{-8\pi^2\sigma^2\Delta T^2}\cos\left(\varphi_A-\varphi_B\right)-\cos\left(\varphi_0+\varphi_A+\varphi_B\right)\right) \qquad (6.11)\\
\langle I_{--}\rangle &= 2A_0^4\left(2+2e^{-2\pi^2\sigma^2\Delta T^2}\cos\left(\frac{\varphi_0}{2}+\varphi_A\right)-2e^{-2\pi^2\sigma^2\Delta T^2}\cos\left(\frac{\varphi_0}{2}+\varphi_B\right)\right.\\
&\quad \left.-e^{-8\pi^2\sigma^2\Delta T^2}\cos\left(\varphi_A-\varphi_B\right)-\cos\left(\varphi_0+\varphi_A+\varphi_B\right)\right) \qquad (6.12)\\
\langle I_{+-}\rangle &= 2A_0^4\left(2-2e^{-2\pi^2\sigma^2\Delta T^2}\cos\left(\frac{\varphi_0}{2}+\varphi_A\right)-2e^{-2\pi^2\sigma^2\Delta T^2}\cos\left(\frac{\varphi_0}{2}+\varphi_B\right)\right.\\
&\quad \left.+e^{-8\pi^2\sigma^2\Delta T^2}\cos\left(\varphi_A-\varphi_B\right)+\cos\left(\varphi_0+\varphi_A+\varphi_B\right)\right) \qquad (6.13)\\
\langle I_{-+}\rangle &= 2A_0^4\left(2+2e^{-2\pi^2\sigma^2\Delta T^2}\cos\left(\frac{\varphi_0}{2}+\varphi_A\right)+2e^{-2\pi^2\sigma^2\Delta T^2}\cos\left(\frac{\varphi_0}{2}+\varphi_B\right)\right.\\
&\quad \left.+e^{-8\pi^2\sigma^2\Delta T^2}\cos\left(\varphi_A-\varphi_B\right)+\cos\left(\varphi_0+\varphi_A+\varphi_B\right)\right). \qquad (6.14)
\end{aligned}$$

As we are interested in the probabilities to measure correlated P_c or anticorrelated P_a detector clicks, we have to sum up the averaged correlations $\langle I_{++}\rangle$ and $\langle I_{--}\rangle$, or $\langle I_{+-}\rangle$ and $\langle I_{-+}\rangle$, respectively. To obtain normalized probabilities, we need to divide by the sum

of all correlations:

$$P_c = \frac{\langle I_{++}\rangle + \langle I_{--}\rangle}{\langle I_{++}\rangle + \langle I_{--}\rangle + \langle I_{+-}\rangle + \langle I_{-+}\rangle} = \frac{1}{4}\left(2 - e^{-8\pi^2\sigma^2\Delta T^2}\cos\left(\varphi_A - \varphi_B\right) - \cos\left(\varphi_0 + \varphi_A + \varphi_B\right)\right)$$
$$\overset{\sigma\Delta T \gg 1}{\approx} \frac{1}{2}\left(1 - \frac{1}{2}\cos\left(\varphi_0 + \varphi_A + \varphi_B\right)\right) \tag{6.15}$$

$$P_a = \frac{\langle I_{+-}\rangle + \langle I_{-+}\rangle}{\langle I_{++}\rangle + \langle I_{--}\rangle + \langle I_{+-}\rangle + \langle I_{-+}\rangle} = \frac{1}{4}\left(2 + e^{-8\pi^2\sigma^2\Delta T^2}\cos\left(\varphi_A - \varphi_B\right) + \cos\left(\varphi_0 + \varphi_A + \varphi_B\right)\right)$$
$$\overset{\sigma\Delta T \gg 1}{\approx} \frac{1}{2}\left(1 + \frac{1}{2}\cos\left(\varphi_0 + \varphi_A + \varphi_B\right)\right). \tag{6.16}$$

We used that $\sigma\Delta T \gg 1$ which follows from $\sigma \sim {}^1/_{T_s}$ and $\Delta T \gg T_s$. Assigning the value -1 to the detectors D_{A-} and D_{B-}, and the value $+1$ to the detectors D_{A+} and D_{B+}, we can compute the averages of the "weighted intensities" measured at the detectors in the right (A) and left (B) arms. By doing so, a positive average means that the intensity at the detector with the plus label is larger. Conversely, a negative average means that the intensity at the detector with the minus label is larger. We obtain

$$E_A = \frac{\langle I_{++}\rangle + \langle I_{+-}\rangle - \langle I_{--}\rangle - \langle I_{-+}\rangle}{\langle I_{++}\rangle + \langle I_{--}\rangle + \langle I_{+-}\rangle + \langle I_{-+}\rangle} \approx 0 \tag{6.17}$$

$$E_B = \frac{\langle I_{++}\rangle + \langle I_{-+}\rangle - \langle I_{+-}\rangle - \langle I_{--}\rangle}{\langle I_{++}\rangle + \langle I_{--}\rangle + \langle I_{+-}\rangle + \langle I_{-+}\rangle} \approx 0, \tag{6.18}$$

where we used $\sigma\Delta T \gg 1$ again. That the averages are approximately zero means that the averaged intensities measured in the detectors are roughly the same. So there is no (visible) single-photon interference in the unbalanced Mach-Zehnder interferometer if the uncertainty in the frequency is large enough such that $\sigma\Delta T \gg 1$ is satisfied. For the correlation coefficient, however, we obtain

$$C = \frac{\langle I_{++}\rangle + \langle I_{--}\rangle - \langle I_{+-}\rangle - \langle I_{-+}\rangle}{\langle I_{++}\rangle + \langle I_{--}\rangle + \langle I_{+-}\rangle + \langle I_{-+}\rangle} - E_A E_B = -\frac{1}{2}\cos\left(\varphi_0 + \varphi_A + \varphi_B\right), \tag{6.19}$$

which means that fourth-order interference is observable even in the classical description, but only with a visibility of

$$\mathcal{V} = \frac{P_{c,\max} - P_{c,\min}}{P_{c,\max} + P_{c,\min}} = \frac{1}{2}, \tag{6.20}$$

where $P_{c,\max}$ ($P_{c,\min}$) is the maximal (minimal) value attainable for P_c depending on φ_A and φ_B.

6.1.2 Quantum Theoretical Description

The quantum mechanical calculation presented here is based on the calculations done by Howell in Ref. [100].

The transformations of the photon creation operators for the modes in the right arm

$(a_0^\dagger(t))$ and the left arm $(b_0^\dagger(t))$ during the setup are given by

$$\begin{aligned} a_0^\dagger(t) &\mapsto \frac{1}{\sqrt{2}}\left(a_u^\dagger(t) + ia_l^\dagger(t)\right) \mapsto \frac{1}{\sqrt{2}}\left(a_u^\dagger(t) + ie^{i\varphi_A + 2\pi i f^- \Delta T} a_l^\dagger(t+\Delta T)\right) \\ &\mapsto \frac{1}{2}\left(a_+^\dagger(t) + ia_-^\dagger(t) + e^{i\varphi_A + 2\pi i f^- \Delta T}\left(ia_-^\dagger(t+\Delta T) - a_+^\dagger(t+\Delta T)\right)\right) \qquad (6.21) \\ b_0^\dagger(t) &\mapsto \frac{1}{\sqrt{2}}\left(b_u^\dagger(t) + ib_l^\dagger(t)\right) \mapsto \frac{1}{\sqrt{2}}\left(b_u^\dagger(t) + ie^{i\varphi_B + 2\pi i f^+ \Delta T} b_l^\dagger(t+\Delta T)\right) \\ &\mapsto \frac{1}{2}\left(b_-^\dagger(t) + ib_+^\dagger(t) + e^{i\varphi_B + 2\pi i f^+ \Delta T}\left(ib_+^\dagger(t+\Delta T) - b_-^\dagger(t+\Delta T)\right)\right) \qquad (6.22) \end{aligned}$$

where the intermediate creation operators $a_u^\dagger(t)$ and $a_l^\dagger(t)$ represent the modes in the upper and lower arms of the unbalanced Mach-Zehnder interferometer ($b_u^\dagger(t)$ and $b_l^\dagger(t)$ accordingly). The final creation operators $a_+^\dagger(t)$ and $a_-^\dagger(t)$ denote the output modes of the second beam splitter directed to the detectors D_{A+} and D_{A-}, respectively (and accordingly for $b_+^\dagger(t)$ and $b_-^\dagger(t)$). Due to the time delays in the lower arms of the Mach-Zehnder interferometer, the operators $a_l^\dagger(t+\Delta T)$ and $b_l^\dagger(t+\Delta T)$ create modes by a time ΔT later than the operators $a_u^\dagger(t)$ and $b_u^\dagger(t)$ at the beam splitter.

The state $|\Psi\rangle$ of the two-photon system after the second beam splitters is then given by

$$\begin{aligned} |\Psi\rangle = \frac{1}{4}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} \mathrm{d}t_1\mathrm{d}t_2 A(|t_1-t_2|)\left(a_+^\dagger(t_1) + ia_-^\dagger(t_1) + e^{i\varphi_A + 2\pi i f^- \Delta T}\left(ia_-^\dagger(t_1+\Delta T) - a_+^\dagger(t_1+\Delta T)\right)\right) \\ \times\left(b_-^\dagger(t_2) + ib_+^\dagger(t_2) + e^{i\varphi_B + 2\pi i f^+ \Delta T}\left(ib_+^\dagger(t_2+\Delta T) - b_-^\dagger(t_2+\Delta T)\right)\right)|00\rangle. \qquad (6.23) \end{aligned}$$

Here, $|00\rangle$ denotes the vacuum on the right and left side in the Fock spaces $\mathcal{H}_A = \bigoplus_{k=0}^{\infty}\mathcal{H}_{A,k}$ and $\mathcal{H}_B = \bigoplus_{k=0}^{\infty}\mathcal{H}_{B,k}$ where $\mathcal{H}_{A,k}$ and $\mathcal{H}_{B,k}$ are the k-particle Hilbert spaces. The function $A(|t_1-t_2|)$ gives the amplitude for the modes being created with a time difference $|t_1-t_2|$.

Using the bosonic commutation relations $[a_i(t), a_j^\dagger(t')] = \delta_{ij}\delta(t-t')$ and $[b_i(t), b_j^\dagger(t')] = \delta_{ij}\delta(t-t')$ with $i,\, j \in \{+,-\}$, we can compute

$$\begin{aligned} a_+(t+\tau)b_+(t)|\Psi\rangle &= \frac{1}{4}\int_{-\infty}^{\infty}\int_{-\infty}^{\infty} \mathrm{d}t_1\mathrm{d}t_2 A(|t_1-t_2|)\left(\delta(t_1-t-\tau) - e^{i\varphi_A + 2\pi i f^- \Delta T}\delta(t_1+\Delta T-t-\tau)\right) \\ &\qquad \times\left(i\delta(t_2-t) + ie^{i\varphi_B + 2\pi i f^+ \Delta T}\delta(t_2+\Delta T-t)\right)|00\rangle \\ &= \frac{1}{4}\int_{-\infty}^{\infty} \mathrm{d}t_1\left(\delta(t_1-t-\tau) - e^{i\varphi_A + 2\pi i f^- \Delta T}\delta(t_1+\Delta T-t-\tau)\right) \\ &\qquad \times\left(iA(|t_1-t|) + ie^{i\varphi_B + 2\pi i f^+ \Delta T}A(|t_1-t+\Delta T|)\right)|00\rangle \\ &= \frac{i}{4}\Big(e^{i\varphi_B + 2\pi i f^+ \Delta T}A(|\tau+\Delta T|) - e^{i\varphi_A + 2\pi i f^- \Delta T}A(|\tau-\Delta T|) \\ &\qquad + A(|\tau|) - e^{i(\varphi_A+\varphi_B) + 4\pi i f_0 \Delta T}A(|\tau|)\Big)|00\rangle. \qquad (6.24) \end{aligned}$$

If we assume that $\Delta T \gg |\tau|$ and that $A(|t|)$ is peaked around zero, i.e., $A(|\Delta T|)$ is approximately zero, we can simplify Eq. (6.24) to obtain

$$a_+(t+\tau)b_+(t)|\Psi\rangle \approx \frac{i}{4}A(|\tau|)\left(1-e^{i(\varphi_A+\varphi_B)+4\pi i f_0\Delta T}\right)|00\rangle, \tag{6.25}$$

and similarly

$$a_-(t+\tau)b_-(t)|\Psi\rangle \approx \frac{i}{4}A(|\tau|)\left(1-e^{i(\varphi_A+\varphi_B)+4\pi i f_0\Delta T}\right)|00\rangle \tag{6.26}$$

$$a_+(t+\tau)b_-(t)|\Psi\rangle \approx -\frac{1}{4}A(|\tau|)\left(1+e^{i(\varphi_A+\varphi_B)+4\pi i f_0\Delta T}\right)|00\rangle \tag{6.27}$$

$$a_-(t+\tau)b_+(t)|\Psi\rangle \approx -\frac{1}{4}A(|\tau|)\left(1+e^{i(\varphi_A+\varphi_B)+4\pi i f_0\Delta T}\right)|00\rangle. \tag{6.28}$$

We are interested in coincidences within a window $|\tau| \ll \Delta T$ as these coincidences correspond to the cases where the photons travel either both along the long or both along the short arms. As A is (sharply) peaked around zero, the probability for the photons being created with a time difference of ΔT within the source is approximately zero. Thus, our assumptions are justified. Now we can use the two-particle correlation functions to compute the coincidences of measurements within the time window $|\tau|$

$$c_{++}(\tau) = \langle\Psi|b_+^\dagger(t)a_+^\dagger(t+\tau)a_+(t+\tau)b_+(t)|\Psi\rangle = \frac{|A(|\tau|)|^2}{8}\left(1-\cos\left(\varphi_A+\varphi_B+\varphi_0\right)\right) \tag{6.29}$$

$$c_{--}(\tau) = \langle\Psi|b_-^\dagger(t)a_-^\dagger(t+\tau)a_-(t+\tau)b_-(t)|\Psi\rangle = \frac{|A(|\tau|)|^2}{8}\left(1-\cos\left(\varphi_A+\varphi_B+\varphi_0\right)\right) \tag{6.30}$$

$$c_{+-}(\tau) = \langle\Psi|b_-^\dagger(t)a_+^\dagger(t+\tau)a_+(t+\tau)b_-(t)|\Psi\rangle = \frac{|A(|\tau|)|^2}{8}\left(1+\cos\left(\varphi_A+\varphi_B+\varphi_0\right)\right) \tag{6.31}$$

$$c_{-+}(\tau) = \langle\Psi|b_+^\dagger(t)a_-^\dagger(t+\tau)a_-(t+\tau)b_+(t)|\Psi\rangle = \frac{|A(|\tau|)|^2}{8}\left(1+\cos\left(\varphi_A+\varphi_B+\varphi_0\right)\right), \tag{6.32}$$

where $\varphi_0 = 4\pi f_0\Delta T$. We can also choose a negative τ (such that the detector at the right side clicks first within the time window) since operators $a_i(t)$ and $b_j(t)$ $i,j \in \{+,-\}$ commute and A depends only on the absolute value of τ. Thus we get the same dependence as given in Eqs. (6.29) - (6.32) for a negative τ. Using the same convention as before where the value -1 is assigned to the detectors D_{A-} and D_{B-}, and the value $+1$ is assigned to the detectors D_{A+} and D_{B+}, we obtain for the single-particle averages of coincidence counts E_a for the detectors on the right side (A) and E_b for the detectors on the left side (B)

$$E_a = \frac{c_{++}(\tau)+c_{+-}(\tau)-c_{-+}(\tau)-c_{--}(\tau)}{c_{++}(\tau)+c_{+-}(\tau)+c_{-+}(\tau)+c_{--}(\tau)} = 0 \tag{6.33}$$

$$E_b = \frac{c_{++}(\tau)+c_{-+}(\tau)-c_{+-}(\tau)-c_{--}(\tau)}{c_{++}(\tau)+c_{+-}(\tau)+c_{-+}(\tau)+c_{--}(\tau)} = 0. \tag{6.34}$$

The correlation coefficient for $|\tau| \ll \Delta T$ is then given by

$$C = \frac{c_{++}(\tau)+c_{--}(\tau)-c_{+-}(\tau)-c_{-+}(\tau)}{c_{++}(\tau)+c_{--}(\tau)+c_{+-}(\tau)+c_{-+}(\tau)} - E_aE_b = -\cos(\varphi_A+\varphi_B+\varphi_0). \tag{6.35}$$

The normalized probabilities to measure correlated P_c or anticorrelated P_a detector clicks can be computed as follows:

$$P_c = \frac{c_{++}(\tau) + c_{--}(\tau)}{c_{++}(\tau) + c_{+-}(\tau) + c_{-+}(\tau) + c_{--}(\tau)} = \frac{1}{2}\left(1 - \cos\left(\varphi_A + \varphi_B + \varphi_0\right)\right) \tag{6.36}$$

$$P_a = \frac{c_{-+}(\tau) + c_{+-}(\tau)}{c_{++}(\tau) + c_{+-}(\tau) + c_{-+}(\tau) + c_{--}(\tau)} = \frac{1}{2}\left(1 + \cos\left(\varphi_A + \varphi_B + \varphi_0\right)\right). \tag{6.37}$$

So in the quantum mechanical description we obtain for the visibility

$$\mathcal{V} = \frac{P_{c,\max} - P_{c,\min}}{P_{c,\max} + P_{c,\min}} = 1, \tag{6.38}$$

where $P_{c,\max}$ ($P_{c,\min}$) is like before the maximal (minimal) value attainable for P_c depending on φ_A and φ_B.

6.2 Simulation of the Franson-Interferometer Experiment

In this section, we employ the discrete-event simulation approach to reproduce the quantum mechanical results derived in the previous section for energy-time entangled photons. We aim at showing that the discrete-event simulation is capable of reproducing the quantum theoretical result of the Franson-interferometer experiment. Moreover, we demonstrate that making use of postselection offers a way to achieve these quantum mechanical results from data obtained from the discrete-event simulation which is purely classical and exhibits no quantum features such as entanglement. The problem is similar to the Einstein-Podolsky-Rosen-Bohm (EPRB) experiment with polarization entangled photons or spin 1/2-particles which has been already simulated [10]. The differences are that here the correlation of the photons originates from the frequencies instead of the polarization, and as we want to observe interference, we have to use the adaptive detectors with learning machine because due to the fluctuating frequencies, linear elements like the beam splitters do not produce interference patterns.

The simulation is based on the setup given in Fig. 6.1. The source creates two messengers with frequencies $f_0 \pm \nu$, where ν is chosen at random from the distribution given in Eq. (6.1), and $f_0 = 327\,500\,\text{GHz}$. The uncertainty σ in Eq. (6.1) is $\sigma = 42\,500\,\text{GHz}$. The values for f_0 and σ are selected similarly to the experiment reported in Ref. [95].

We generate $k = 200$ data points where for each data point the parameter ξ of the polarization, and the initial phases ψ_1 and ψ_2 of the messengers are chosen uniformly at random from $[0, 2\pi)$ for both messengers. The phase shifts φ_A and φ_B are also chosen at random between 0 and 2π anew for each data point. For each data point, $N = 500\,000$ messengers with the same parameters ξ, ψ_1, ψ_2, φ_A, and φ_B are generated. The variation in the frequencies ν is updated every $N_\nu = 100$ events such that the fluctuating frequencies cause decoherence, and the first-order interference vanishes.

After the generation of the messengers, each of them is transformed by their own devices, i.e., the devices in the right (left) arm of the interferometer get information only from one of the two messengers. Due to the fluctuating source, we can use the simple beam splitters described in section 2.5, and for the phase shifters we use the

transformation mentioned in section 2.4. The detectors are the most sophisticated devices in this simulation. Basically, we use the detectors with the learning machines introduced in section 2.6. In addition, we let the detectors change the detection time of the messengers. As we are interested only in the difference of the detection time, we first set the creation time of the messengers to zero. Then, the messengers collect time delays if they travel along the long arm of their unbalanced Mach-Zehnder interferometer. This time delay due to the different lengths of the interferometer arms is chosen to be $\Delta T = 2\,\mathrm{ns}$ which is a typical value according to [100]. From $f_0 \Delta T = 655\,000$ it follows that $\varphi_0 = 4\pi f_0 \Delta T$ is a multiple of 2π and we can neglect it in Eqs. (6.36) and (6.37). In our time delay model of the detector, the time delay t_d depends on the internal state of the detector, i.e., on the vector $\mathbf{Y}$:

$$t_d = -T_0 \left(1 - ||\mathbf{Y}||\right)^v \log\left(r\right), \tag{6.39}$$

where the parameters T_0 and v have to be chosen appropriately, and $r \in [0, 1)$ is a random number drawn anew for each messenger from a uniform distribution. The model for the time delay was already introduced in Ref. [15]. We find that we can select the parameters of this time delay model such that we obtain satisfactory results. Basically, the model generates random time delays according to an exponential distribution where the mean is a function of the detector's internal state $\mathbf{Y}$ which is affected by the incoming messages.

After trying various values for T_0 and v, we finally decided to use $T_0 = 400\,\mathrm{ns}$ and $v = 2$ for both detectors. So the detectors add a random time delay to the messengers and possibly produce a click, i.e., a one, or no click, i.e., a zero. If both detectors return a one, the difference in the times of the messengers is computed and compared with the time window τ which we set to $\tau = 0.033\,\mathrm{ns}$. If the absolute value of the time difference is smaller than the time window τ, the event is counted as a coincidence, otherwise it is discarded. In case of a coincidence, the event contributes to one of the counters `c_pp`, `c_pm`, `c_mp` or `c_mm` which correspond to the two-particle correlation functions c_{++}, c_{+-}, c_{-+}, and c_{--} that we need to compute the probabilities P_c and P_a, the averages E_a and E_b, and the correlation coefficient C.

The results are shown in Fig. 6.2 and Fig. 6.3. For the chosen set of parameters, the results are in excellent agreement with the quantum mechanical description, and in the cases of the correlation coefficient C and the probabilities P_c and P_a, exceed the prediction of the classical calculation. In Fig. 6.2, the results of the probabilities P_c and P_a are visualized, and the sinusoidal shape as a function of $\varphi_A + \varphi_B$ is clearly observable. Thus, we achieved fourth-order interference with the visibility being close to the one predicted by quantum theory. The plots of the correlation coefficient C and the single-particle expectation values E_a and E_b dependent on $\varphi_A + \varphi_B$ are depicted in Fig. 6.3. The expectation values are nearly zero and fluctuate statistically about zero which means that the detectors D_{A+} and D_{A-} (D_{B+} and D_{B-} as well) click with approximately equal probability, i.e., no single-particle interference occurs.

Hence, the discrete-event simulation is capable of reproducing the quantum theoretical prediction for the fourth-order interference of energy-time entangled photons although the discrete-events simulation is classical in the sense that the messengers' trajectories are always well-defined, and the simulation method satisfies Einstein's criterion of locality.

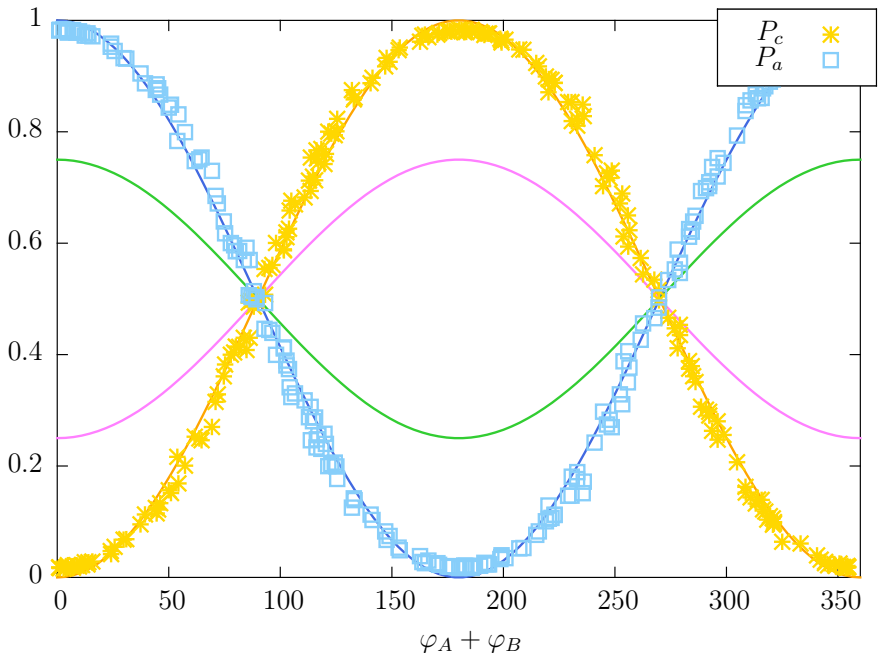

Figure 6.2: Probabilities to measure correlated (P_c) or anticorrelated (P_a) coincidences dependent on the sum of the phase shifts $\varphi_A + \varphi_B$. The theoretical, quantum mechanical results are represented by the orange and dark blue lines, respectively. The classical expectation is visualized by the pink and green lines. Stars and squares represent the simulation results. For each data point, $N = 500\,000$ events are generated. The time window is set to $\tau = 0.033\,\text{ns}$, and the detector's learning parameter is set to $\gamma = 0.6$.

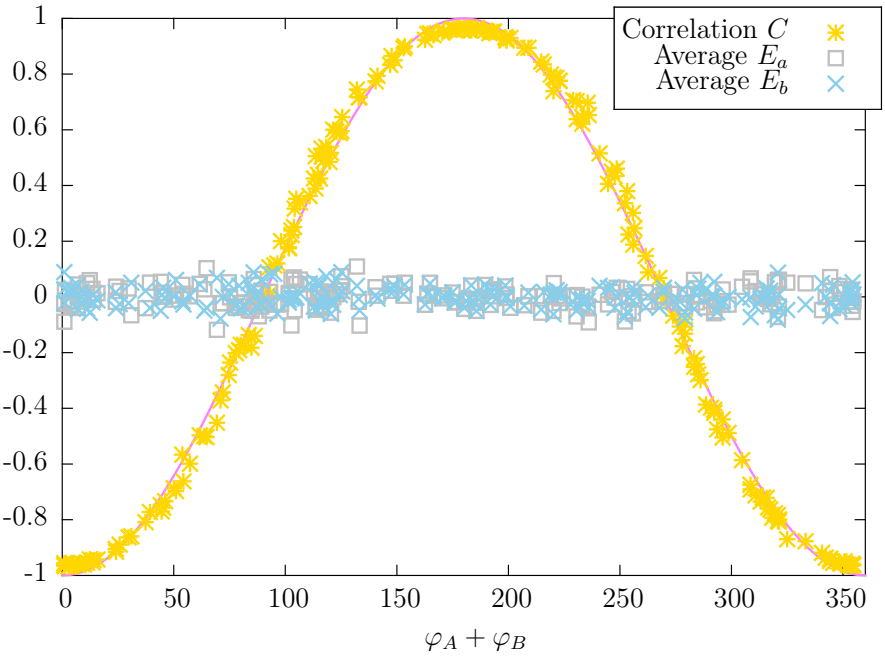

Figure 6.3: Correlation coefficient C and single-particle averages E_a and E_b dependent on the sum of the phase shifts $\varphi_A + \varphi_B$. The parameters N, τ, and γ are the same as in Fig. 6.2. The pink line represents the quantum theoretical result.

Conclusion

In this chapter, we have shown that we can reproduce the quantum theoretical predictions for the Franson-interferometer with the discrete-event simulation. In quantum theory, the photon states in the Franson-interferometer experiment can be described as energy-time entangled states. Postselection then leads to the visibility of the fourth-order interference attaining the value 1. Here, we have demonstrated that we are capable of reproducing the quantum mechanical predictions with postselection of events generated by a discrete-event simulation. The generation of these events has nothing to do with entanglement, nevertheless the results coincide with the quantum theoretical description.

7 Summary

In this thesis, we utilized the discrete-event simulation method to simulate experiments of quantum walks, quantum key distribution, the Franson-interferometer, and factoring.

To simulate quantum phenomena, usually the Schrödinger equation is solved numerically. For discrete-event simulations of quantum phenomena, neither the time-dependent Schrödinger equation nor the wave equation needs to be solved. The method which we discussed in chapter 2 is based on the simulation of single particles moving through an experimental setup of distinct devices. The devices affect the internally stored states of the particles called messages which may then influence whether and where the particles are finally detected. In turn, the internal states of the particles affect some of the devices, namely those containing a learning machine, usually the beam splitters or detectors. Through this mechanism, particles can influence the path taken by the following particles and finally lead to interference. However, the particles cannot communicate directly with each other as there is always only one particle in (its part of) the setup. Moreover, these simulated particles have well-defined trajectories. Thus, they satisfy Einstein's criteria of realism and local causality. Nonetheless, discrete-event simulations are capable of reproducing quantum mechanical predictions.

We used this method to reproduce and investigate the results of experiments which show quantum phenomena. We focused on experiments performing quantum walks and quantum key distribution, but also simulated the Franson-interferometer and a proposal by Summhammer for factoring with a network of Mach-Zehnder interferometers.

We examined that proposal for factoring in chapter 3 in three steps: First, we had a look at the basic idea of three consecutively arranged Mach-Zehnder interferometers with changing phase differences to check three numbers for being factors. This turned out to work, but not perfectly well. So already the basic idea did not work as well as expected. The intensity patterns, which were measured at the detectors and were to be used to decide whether a factor was included in the tested numbers, sometimes deviated a lot from the intensities in the table given in the proposal. Nevertheless, the discrete-event simulation could reproduce the intensity patterns that could be computed exactly without using the approximations made in the proposal.

Second, we investigated a straightforward but also somewhat incomplete version to parallelize the check for factors, and third, we examined the version for parallelization given in the proposal. The straightforward version is just an extension of the basic idea such that at each output arm of a Mach-Zehnder interferometer, additional Mach-Zehnder interferometers were placed until there were always three in succession. Because in this arrangement there were no modifications in the detection scheme, it was possible that no particles were passing through some of the interferometers. As a result, sometimes not all numbers were checked for being factors. Nevertheless, at least one factor could be determined whenever at least one was included in the tested numbers. However, as for the basic idea, the intensity patterns of the simulation and exact evaluation (which matched very well) differed from the look-up table which was obtained by applying approximations

to get rid of the dependence on the tested numbers.

The more complex way for parallelization given in the proposal takes into account that at some times no particles are passing through some of the interferometers. It circumvents this fact by delaying the changes of the phase differences and measuring the intensities at different stages. The construction of the general look-up table then required more approximations which led to even larger deviations from the exact evaluation. The results obtained by the discrete-event simulation and the exact evaluation coincided well. However, due to the approximations the look-up table that was to be used to determine which numbers were actually factors deviated a lot from the measured intensities, thereby making the distinction of the patterns difficult. So for this experiment, we found that the discrete-event simulation is capable of reproducing the theoretical results, but we could not be convinced of the applicability of the setup in order to obtain the factors of a given number.

After a short discussion of the random walk, we started with the investigation of the quantum walk in chapter 4. As for the random walk, a particle is moved to the left or to the right, but for the quantum walk the direction depends on some degree of freedom of the particle, e.g., the polarization in case of a photon. If this degree of freedom is in a superposition state, the particle's position state is in a superposition of being moved to the left and to the right. Applying a Hadamard transformation to the degree of freedom and then moving the particle again leads to interference effects for more than two movements. Thus, the probability to detect the particle at a certain detector complies with a distribution which originates from interference.

We investigated and simulated two different experiments implementing the quantum walk. The first one was implemented with a network of beam splitters and phase shifters only, but here, in contrast to the factoring experiments, we implemented a variable number of levels in the simulation. The comparison of the analytical results of the quantum walk and the results obtained from the discrete-event simulation showed that we are capable of reproducing the probability distribution of the quantum walk by means of the discrete-event simulation which is in a sense purely classical.

Depending on the phase difference induced by the phase shifters, we could control the symmetry of the quantum walk as could the experimentalists. We also validated that for asymmetric quantum walks the mean value of the position can deviate from zero, which is the mean value of the position for the random walk if zero was the initial position. What also distinguishes the quantum walk from the random walk is the growth of the variance of the position. For the random walk, the variance of the position grows linearly, whereas for the quantum walk we could confirm that the variance of the position grows approximately quadratically.

In the second experiment which we examined regarding the quantum walk, the quantum walk is shown to violate the Leggett-Garg inequality which we also discussed briefly. As this experiment was performed with atoms, we had to adapt the setup such that we could simulate this experiment as if it was done with photons. For the simulation of this setup we had to apply polarizing beam splitters and half-wave plates. First, we simulated the experiment for three different runs. In this way we could reproduce the same results as the experimental group, i.e., we found a violation of the Leggett-Garg inequality which is supposed to indicate that "macroscopic realism" and "non-invasive measurability" cannot both be satisfied. As the group claimed to have achieved "non-invasive measurability", they concluded that the quantum walk does not satisfy "macroscopic realism".

Therefore, as a second test, we performed the same steps with the random walk. However, we found that in this case, the Leggett-Garg inequality was satisfied. In the experiment, particles have been discarded to obtain the data that brought about the violation of the Leggett-Garg inequality. So we changed the way of gathering the data by adding a label of the particles' positions. In the simulation we could do this without inducing disturbances, and thus measure the particles' positions non-invasively. In this way, we could obtain all necessary data from a single run, and this data finally did not violate the Leggett-Garg inequality. Thus, we could show that the violation of the Leggett-Garg inequality was caused by the discarding and mingling of data of different runs which is still effectively an invasive measurement. In the simulation, we did not need to do so as we could easily perform a non-invasive measurement, and hence we did not achieve a violation of the Leggett-Garg inequality with the data of the quantum walk from a single run. So we can conclude that the quantum walk in the simulation satisfied "non-invasive measurability" as well as "macroscopic realism", but in the experiment the group did not achieve "non-invasive measurability". Thus, they cannot make a statement about whether or not their experiment of the quantum walk satisfied "macroscopic realism".

Next, in chapter 5 we had a look at quantum key distribution. First, we discussed classical cryptography, where "classical" refers to the nowadays used techniques not involving quantum mechanics. Summarizing, the problem of classical cryptography is either that the security is based on assumptions of computational hardness (like for factoring in the case of RSA), or that cryptosystems which are unconditionally secure are so inconvenient to use due to the complicated key handling that they are not applicable for everyday use (like the one-time pad).

Then we discussed in more detail the first quantum key distribution protocol (the BB84 protocol), which promises in theory a secure way of exchanging a key for the one-time pad. The basic idea of the protocol is that Alice sends photons at random in one of four polarization states of two conjugate bases and Bob measures the polarization in one of the two bases at random. By comparing the chosen bases and discarding the measurements where they used different ones, they know they agree on the remaining polarizations without the need of announcing them. In that way, they can secretly acquire a string of shared bits which they obtain from the two polarization states of each basis. Due to the use of conjugate bases and the no-cloning theorem, they can detect any eavesdropper by comparing parts of their measured polarizations. Unfortunately, in reality the protocol is not as secure as in theory due to imperfections in the implementations.

Subsequently, we reviewed the progress of quantum key distribution made in the last years regarding security issues due to these imperfect implementations and proposals for improvement. Finally, we considered one of the recent quantum key distribution experiments in which security is based on measurements of parities only. The performed measurements are single-photon Bell-state measurements where the two qubits are represented by two degrees of freedom of the same photon.

We simulated this experiment by using the discrete-event simulation method. Again we utilized the implementations of beam splitters and phase shifters, but we had to use a different kind of implementation for the detectors than before as in this setup time played an important role. For this reason, we had to simulate a fluctuating source which sent photons with various frequencies. Due to the varying frequencies, the coherence, which is needed for interference to occur at linear optical elements such as beam splitters, was destroyed. Thus, interference had to originate from the only non-linear elements used in

the setup, namely the detectors.

We could reproduce the same functional dependence of the Bell-state measurement outcomes on the setting of the phase shifters as in the experiment. We could use these relations to generate a key. So we were able to reproduce the correlations assigned to Bell states which are described by entanglement in quantum theory. Although the discrete-event simulation comes without the need of quantum theory and entanglement, we achieved a replication of these correlations for the simulated particles.

The next experiment investigated in chapter 6 was the Franson-interferometer experiment, which is sometimes also applied to quantum key distribution. The aim of the experiment itself is the measurement of the quantum mechanical visibility of the fourth-order interference of energy-time entangled photons originating from a two-photon source, for example a crystal realizing parametric down-conversion, without measuring single-photon interference. The photons produced by the source pass through one of two unbalanced Mach-Zehnder interferometers and are detected by one of four detectors. Only coincidences are counted, i.e., two of the detectors, one at each Mach-Zehnder interferometer, have to produce a click within a certain time window for the event to be registered. Then the correlations of the detected events are computed pairwise for one detector of each interferometer for observing the fourth-order interference depending on the phase shifts that were set up in the unbalanced Mach-Zehnder interferometers.

We computed the expected visibilities of the fourth-order interferences for classical wave theory and within quantum theory. The visibility in the quantum mechanical case is twice as large as in the classical theory. In the simulation we had to add a time tag model such that we could discard non-coincident events to obtain the quantum mechanical visibility. Because time again had to be considered explicitly, and for the entangled photons in this experiment the frequencies were supposed to cover a relatively large spectrum, the simulated source also generated photons with fluctuating frequencies. We used the detectors with learning machine to obtain the interference pattern. The time-tag model caused random delays in the detectors, partly depending on the photons' stored messages. In this way, we have been able to reproduce the quantum mechanical prediction with the discrete-event simulation method. The correlation leading to the observable fourth-order interference is described by energy-time entanglement in quantum theory, but we could reproduce these results without making use of entanglement or wave functions. Only the postselection of events based on coincidences in time was needed to achieve the quantum mechanical result.

In conclusion, we could apply the discrete-event simulation to all investigated quantum mechanical experiments and reproduce the results of the experimental implementations and the predictions of the theoretical descriptions. Although we did not solve the time-dependent Schrödinger equation or another wave equation, but used the discrete-event simulation method which satisfies Einstein's criteria of local causality and realism, we were still able to observe quantum effects such as interference and correlations associated with entanglement.

Bibliography

[1] J. Hardy, Y. Pomeau, and O. de Pazzis, *Time evolution of a two-dimensional model system. I. Invariant states and time correlation functions*, J. Math. Phys. **14**, 1746 (1973).

[2] A. Adamatzky (Ed.), *Game of Life Cellular Automata*, Springer (2010) ISBN 978-1-84996-216-2.

[3] D. Home, *Conceptual Foundations of Quantum Physics*, Springer (1997) ISBN 978-1-4757-9810-4

[4] L. E. Ballentine, *The Statistical Interpretation of Quantum Mechanics*, Rev. Mod. Phys. **42**, 358 (1970).

[5] D. Bohm, *A Suggested Interpretation of the Quantum Theory in Terms of "Hidden" Variables. I*, Phys. Rev. **85**, 166 (1952).

[6] D. Bohm, *A Suggested Interpretation of the Quantum Theory in Terms of "Hidden" Variables. II*, Phys. Rev. **85**, 180 (1952).

[7] H. Everett III, PhD Thesis, long version: *Theory of the Universal Wave Function* (1956), published in J. A. Barrett, and P. Byrne (Eds.) *The Everett Interpretation of Quantum Mechanics: Collected Works 1955-1980 with Commentary*, Princeton University Press (2012) ISBN 978-0691145075.

[8] G. C. Ghirardi, A. Rimini, and T. Weber, *Unified dynamics for microscopic and macroscopic systems*, Phys. Rev. D **34**, 470 (1986).

[9] H. De Raedt, K. De Raedt, and K. Michielsen, *Event-based simulation of single-photon beam splitters and Mach-Zehnder interferometers*, Europhys. Lett. **69**, 861 (2005).

[10] H. De Raedt, K. De Raedt, K. Michielsen, K. Keimpema, and S. Miyashita, *Event-by-Event Simulation of Quantum Phenomena: Application to Einstein-Podolsky-Rosen-Bohm Experiments*, J. Comp. Theor. Nanosci. **4**, 957 (2007).

[11] S. Zhao, and H. De Raedt, *Event-by-Event Simulation of Quantum Cryptography Protocols*, J. Comp. Theor. Nanosci. **5**, 490 (2008).

[12] F. Jin, H. De Raedt, and K. Michielsen, *Event-by-event simulation of the Hanbury Brown-Twiss experiment with coherent light*, Commun. Comput. Phys. **7**, 813 (2010).

[13] B. Trieu, K. Michielsen, and H. De Raedt, *Event-based simulation of light propagation in lossless dielectric media*, Comp. Phys. Commun. **182**, 726 (2011).

[14] K. Michielsen, F. Jin, and H. De Raedt, *Event-based Corpuscular Model for Quantum Optics Experiments*, J. Comp. Theor. Nanosci. **8**, 1052 (2011).

[15] K. Michielsen, F. Jin, M. Delina, and H. De Raedt, *Event-by-event simulation of nonclassical effects in two-photon interference experiments*, Phys. Scr. **T151**, 014005 (2012).

[16] K. Michielsen, and H. De Raedt, *Event-based simulation of quantum physics experiments*, Int. J. Mod. Phys. C **25**, 1430003 (2014).

[17] F. James, *A review of pseudorandom number generators*, Comp. Phys. Commun. **60**, 329 (1990).

[18] M. Matsumoto, and T. Nishimura, *Mersenne Twister: A 623-dimensionally Equidistributed Uniform Pseudo-random Number Generator*, ACM Trans. Model. Comput. Simul. **8**, 3 (1998).

[19] L. Blum, M. Blum and M. Shub, *A simple unpredictable pseudo-random number generator*, SIAM J. Comput. **15**, 364 (1986).

[20] Christopher C. Gerry and Peter L. Knight, *Introductory Quantum Optics*, Cambridge University Press (2005) ISBN 978-0-521-52735-4.

[21] P. W. Shor, *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*, SIAM J. Comput. **26**, 1484 (1997).

[22] J. Summhammer, *Factoring and Fourier transformation with a Mach-Zehnder interferometer*, Phys. Rev. A **56**, 4324 (1997).

[23] H. Jeong, M. Paternostro, and M. S. Kim, *Simulation of quantum random walks using the interference of a classical field*, Phys. Rev. A **69**, 012310 (2004).

[24] C. Robens, W. Alt, D. Meschede, C. Emary, and A. Alberti, *Ideal Negative Measurements in Quantum Walks Disprove Theories Based on Classical Trajectories*, Phys. Rev. X **5**, 011003 (2015).

[25] E. A. Codling, M. J. Plank, and S. Benhamou, *Random walk models in biology*, J. R. Soc. Interface **5** 813 (2008).

[26] P. Bovet, and S. Benhamou, *Spatial Analysis of Animals' Movements Using a Correlated Random Walk Model*, J. theor. Biol. **131**, 419 (1988).

[27] G. van den Engh, R. Sachs, and B. J. Trask, *Estimating genomic distance from DNA sequence location in cell nuclei by a random walk model*, Science **257**, 1410 (1992).

[28] D. J. Aldous, *The Random Walk Construction of Uniform Spanning Trees and Uniform Labelled Trees*, SIAM J. Discrete Math. **3**, 450 (1990).

[29] F. Fouss, A. Pirotte, J.-M. Renders, and M. Saerens, *Random-Walk Computation of Similarities between Nodes of a Graph with Applocation to Collaborative Recommendation*, IEEE Transactions on Knowledge and Data Engineering **19**, 355 (2007).

[30] Y. Aharonov, L. Davidovich, and N. Zagury, *Quantum random walks*, Phys. Rev. A **48**, 1687 (1993).

[31] F. Zähringer, G. Kirchmair, R. Gerritsma, E. Solano, R. Blatt, and C. F. Roos, *Realization of a Quantum Walk with One and Two Trapped Ions*, Phys. Rev. Lett. **104**, 100503 (2010).

[32] Y.-C. Jeong, C. Di Franco, H.-T. Lim, M. S. Kim, and Y.-H. Kim, *Experimental realization of a delayed-choice quantum walk*, Nat. Commun. **4**, 2471 (2013).

[33] W. Dür, R. Raussendorf, V. M. Kendon, and H.-J. Briegel, *Quantum walks in optical lattices*, Phys. Rev. A **66**, 052319 (2002).

[34] M. Karski, L. Förster, J.-M. Choi, A. Steffen, W. Alt, D. Meschede, and A. Widera, *Quantum Walk in Position Space with Single Optically Trapped Atoms*, Science **325**, 174, (2009).

[35] B. C. Travaglione, and G. J. Milburn, *Implementing the quantum random walk*, Phys. Rev. A **65**, 032310 (2002).

[36] H. Schmitz, R. Matjeschk, C. Schneider, J. Glueckert, M. Enderlein, T. Huber, and T. Schaetz, *Quantum Walk of a Trapped Ion in Phase Space*, Phys. Rev. Lett. **103**, 090504 (2009).

[37] B. C. Sanders, and S. D. Bartlett, *Quantum quincunx in cavity quantum electrodynamics*, Phys. Rev. A **67**, 042305 (2003).

[38] A. Schreiber, K. N. Cassemiro, V. Potoček, A. Gábris, P. J. Mosley, E. Andersson, I. Jex, and C. Silberhorn, *Photons Walking the Line: A Quantum Walk with Adjustable Coin Operations*, Phys. Rev. Lett. **104**, 050502 (2010).

[39] M. A. Broome, A. Fedrizzi, B. P. Lanyon, I. Kassal, A. Aspuru-Guzik, and A. G. White, *Discrete Single-Photon Quantum Walks with Tunable Decoherence*, Phys. Rev. Lett. **104**, 153602 (2010).

[40] J. Kempe, *Quantum random walks - an introductory overview*, Contemp. Phys. **44**, 307 (2003).

[41] A. J. Leggett, and A. Garg, *Quantum Mechanics versus Macroscopic Realism: Is the Flux There when Nobody Looks?*, Phys. Rev. Lett. **54**, 857 (1985).

[42] H. De Raedt, K. Hess, and K. Michielsen, *Extended Boole-Bell Inequalities Applicable to Quantum Theory*, J. Comp. Theor. Nanosci. 8, 1011 (2011).

[43] Z. Zhao, J. Du, H. Li, T. Yang, Z.-B. Chen, and J.-W. Pan, *Implement Quantum Random Walks with Linear Optics Elements*, quant-ph/0212149v1 (2002).

[44] L. E. Ballentine, *Realism and Quantum Flux Tunneling*, Phys. Rev. Lett. **59**, 1493 (1987).

[45] D. R. Stinson, *Cryptography: Theory and Practice*, CRC Press (2005) ISBN 978-1-58488-508-5.

[46] W. Diffie, and M. E. Hellman, *New directions in cryptography*, IEEE Trans. Inf. Theory **22**, 644 (1976).

[47] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, *Quantum cryptography*, Rev. Mod. Phys. **74**, 145 (2002).

[48] J. Daemen, and V. Rijmen, *AES Proposal: Rijndael*, (1998).

[49] R. L. Rivest, A. Shamir, and L. Adleman, *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, Commun. ACM **21**, 120 (1978).

[50] N. El-Fishawy, and O. M. Abu Zaid, *Quality of Encryption Measurement of Bitmap Images with RC6, MRC6, and Rijndael Block Cipher Algorithms*, International Journal of Network Security **5**, 241 (2007).

[51] C. H. Bennet, and G. Brassard, *Quantum cryptography: Public key distribution and coin tossing*, Proc. of the IEEE Int. Conf. on Computers, Systems & Signal Processing, pp. 175-179 (1984).

[52] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, *Experimental Quantum Cryptography*, J. Cryptology **5**, 3 (1992).

[53] W. K. Wootters, and W. H. Zurek, *A single quantum cannot be cloned*, Nature **299**, 802 (1982).

[54] D. Dieks, *Communication by EPR devices* Phys. Lett. A **92**, 271 (1982).

[55] M. A. Nielsen, and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press (2000) ISBN 978-1-107-00217-3.

[56] C. H. Bennett, G. Brassard, and J.-M. Robert, *Privacy amplification by public discussion*, SIAM J. Comput. **17**, 210 (1988).

[57] R. Renner, N. Gisin, and B. Kraus, *Information-theoretic security proof for quantum-key-distribution protocols*, Phys. Rev. A **72**, 012332 (2005).

[58] D. Mayers, *On the Security of the Quantum Oblivious Transfer and Key Distribution Protocols*, Springer, Advances in Cryptology - CRYPTO '95, LNCS **963**, 124 (1995).

[59] G. Brassard, *Cryptography in a Quantum World*, Springer, SOFSEM 2016: Theory and Practice of Computer Science, LNCS **9587**, 3 (2016).

[60] B. Huttner, N. Imoto, N. Gisin, and T. Mor, *Quantum cryptography with coherent states*, Phys. Rev. A **51**, 1863 (1995).

[61] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, *Limitations on Practical Quantum Cryptography*, Phys. Rev. Lett. **85**, 1330 (2000).

[62] N. Lütkenhaus, and M. Jahma, *Quantum key distribution with realistic states: photon-numer statistics in the photon-number splitting attack*, New J. Phys. **4**, 44 (2002).

[63] W.-Y. Hwang, *Quantum Key Distribution with High Loss: Toward Global Secure Communication* Phys. Rev. Lett. **91**, 057901 (2003).

[64] H.-K. Lo, X. Ma, and K. Chen, *Decoy State Quantum Key Distribution*, Phys. Rev. Lett. **94**, 230504 (2005).

[65] V. Makarov, A. Anisimov, and J. Skaar, *Effects of detector efficiency mismatch on security of quantum cryptosystems*, Phys. Rev. A **74**, 022313 (2006).

[66] B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma, *Time-shift attack in practical quantum cryptosystems*, Quantum Inf. Comput. **7**, 073 (2007).

[67] Y. Zhao, C. H. F. Fung, B. Qi, C. Chen, and H. K. Lo, *Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems*, Phys. Rev. A **78**, 042333 (2008).

[68] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, *Trojan-horse attacks on quantum-key-distribution systems*, Phys. Rev. A **73**, 022320 (2006).

[69] V. Makarov, *Controlling passively quenched single photon detectors by bright light*, New J. Phys. **11**, 065003 (2009).

[70] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, *Hacking commercial quantum cryptography systems by tailored bright illumination*, Nature Photonics **4**, 686 (2010).

[71] V. Scarani, and C. Kurtsiefer, *The black paper of quantum cryptography: Real implementation problems*, Theoretical Computer Science, **560**, 27 (2014).

[72] R. Allèaume, C. Branicard, J. Bouda, T. Debuisschert, M. Dianati, N. Gisin, M. Godfrey, P. Grangier, T. Länger, N. Lütkenhaus, C. Monyk, P. Painchault, M. Peev, A. Poppe, T. Pornin, J. Rarity, R. Renner, G. Ribordy, M. Riguidel, L. Salvail, A. Shields, H. Weinfurter, and A. Zeilinger, *Using quantum key distribution for cryptographic purposes: A survey*, Theoretical Computer Science **560**, 62 (2014).

[73] F. Xu, M. Curty, B. Qi, and H.-K. Lo, *Measurement-Device-Independent Quantum Cryptography*, IEEE Journal of Selected Topics in Quantum Electronics **21**, 148 (2015).

[74] A. Acín, N. Gisin, and L. Masanes, *From Bell's Theorem to Secure Quantum Key Distribution*, Phys. Rev. Lett. **97**, 120405, (2006).

[75] D. Mayers, and A. Yao, *Quantum cryptography with imperfect apparatus*, Proc. 39th Annu. Symp. Found. Comput. Sci., 503 (1998).

[76] D. Mayers, and A. Yao, *Self testing quantum apparatus*, Quantum Inform. Comput. **4**, 273 (2004).

[77] J. Barrett, L. Hardy, and A. Kent, *No Signaling and Quantum Key Distribution*, Phys. Rev. Lett. **95**, 010503, (2005).

[78] H.-K. Lo, M. Curty, and B. Qi, *Measurement-Device-Independent Quantum Key Distribution*, Phys. Rev. Lett. **108**, 130503 (2012).

[79] S. L. Braunstein, and S. Pirandola, *Side-Channel-Free Quantum Key Distribution*, Phys. Rev. Lett. **108**, 130502 (2012).

[80] A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel, *Real-World Two-Photon Interference and Proof-of-Principle Quantum Key Distribution Immune to Detector Attacks*, Phys. Rev. Lett. **111**, 130501 (2013).

[81] Y. Liu, T.-Y. Chen, L.-J. Wang, H. Liang, G.-L. Shentu, J. Wang, K. Cui, H.-L. Yin, N.-L. Liu, L. Li, X. Ma, J. S. Pelc, M. M. Fejer, C.-Z. Peng, Q. Zhang, and J.-W. Pan, *Experimental Measurement-Device-Independent Quantum Key Distribution*, Phys. Rev. Lett. **111**, 130502 (2013).

[82] T. Ferreira da Silva, D. Vitoreti, G. B. Xavier, G. C. do Amaral, G. P. Temporão, and J. P. von der Weid, *Proof-of-principle demonstration of measurement-device-independent quantum key distribution using polarization qubits*, Phys. Rev. A **88**, 052303 (2013).

[83] Z. Tang, Z. Liao, F. Xu, B. Qi, L. Qian, and H.-K. Lo, *Experimental Demonstration of Polarization Encoding Measurement-Device-Independent Quantum Key Distribution*, Phys. Rev. Lett. **112**, 190503 (2014).

[84] C. C. W. Lim, B. Korzh, A. Martin, F. Bussières, R. Thew, and H. Zbinden, *Detector-device-independent quantum key distribution*, Appl. Phys. Lett. **105**, 221112 (2014).

[85] P. González, L. Rebón, T. Ferreira da Silva, M. Figueroa, C. Saavedra, M. Curty, G. Lima, G. B. Xavier, and W. A. T. Nogueira, *Quantum key distribution with untrusted detectors*, Phys. Rev. A **92**, 022337 (2015).

[86] W.-F. Cao, Y.-Z. Zhen, Y.-L. Zheng, Z.-B. Chen, N.-L. Liu, K. Chen, and J.-W. Pan, *Highly Efficient Quantum Key Distribution Immune to All Detector Attacks*, arXiv:1410.2928v1 (2014).

[87] W.-Y. Liang, M. Li, Z.-Q. Yin, W. Chen, S. Wang, X.-B. An, G.-C. Guo, and Z.-F. Han, *Simple implementation of quantum key distribution based on single-photon Bell-state measurement*, Phys. Rev. A **92**, 012319 (2015).

[88] B. Qi, *Trustworthiness of detectors in quantum key distribution with untrusted detectors*, Phys. Rev. A **91**, 020303 (2015).

[89] A. K. Ekert, *Quantum Cryptography Based on Bell's Theorem* Phys. Rev. Lett. **67**, 661 (1991).

[90] L. E. Ballentine, *Quantum Mechanics A Modern Development*, Chapter 19, World Scientific Publishing Co. Pte. Ltd. (1998) ISBN 981-02-4105-4.

[91] J. D. Franson, *Bell Inequality for Position and Time*, Phys. Rev. Lett. **62**, 2205 (1989).

[92] P. G. Kwiat, W. A. Vareka, C. K. Hong, H. Nathel, and R. Y. Chiao, *Correlated two-photon interference in a dual-beam Michelson interferometer*, Phys. Rev. A **41**, 2910 (1990).

[93] Z. Y. Ou, X. Y. Zou, L. J. Wang, and L. Mandel, *Observation of Nonlocal Interference in Separated Photon Channels*, Phys. Rev. Lett. **65**, 321 (1990).

[94] J. D. Franson, *Two-photon interferometry over large distances*, Phys. Rev. A **44**, 4552 (1991).

[95] J. Brendel, E. Mohler, and W. Martienssen, *Time-Resolved Dual-Beam Two-Photon Interferences with High Visibility*, Phys. Rev. Lett. **66**, 1142 (1991).

[96] I. Marcikic, H. de Riedmatten, W. Tittel, H. Zbinden, M. Legré, and N. Gisin, *Distribution of Time-Bin Entangled Qubits over 50 km of Optical Fiber*, Phys. Rev. Lett. **93** 180502 (2004).

[97] T. Inagaki, N. Matsuda, O. Tadanaga, M. Asobe, and H. Takesue, *Entanglement distribution over 300 km of fiber*, Opt. Express **21**, 23241 (2013).

[98] J. Jogenfors, A. M. Elhassan, J. Ahrens, M. Bourennane, and J.-Å. Larsson, *Hacking the Bell test using classical light in energy-time entanglement-based quantum key distribution*, Sci. Adv. **1**, e1500793 (2015).

[99] H. De Raedt, F. Jin, and K. Michielsen, *Note on HOM experiment*, unpublished.

[100] J. C. Howell, *Franson Interference: Space-like separated method for determining time-time correlations of entangled photons*, `http://www.pas.rochester.edu/~howell/mysite2/Tutorials/Franson%20Interference.pdf`.

Acknowledgements

At this point, I would like to thank all the people who contributed in various ways to finishing this thesis. First of all, I thank Kristel Michielsen for affording me the opportunity to write this thesis by providing the topic and accepting to supervise me including a very detailed proofread. She and Hans De Raedt also discussed my results very thoroughly and patiently with me and supported me with good suggestions when I did not know how to proceed, which I am very grateful for. Thank you both for your guidance.

Special thanks go to my boyfriend Dennis Willsch who mostly helped me in finding programming mistakes by asking the right questions, but also for aid in language issues, for discussions not only regarding the topic of my thesis, and of course for being there whenever I needed him.

Next, I would like to thank Fengping Jin for his helpful advice and providing me with instructive material.

Moreover, I thank my family as well as Dennis' family for their interest, encouragement, and support in all the other ways that are not related to physics during the last five years of my study.

Last but not least, I give thanks to my friends Marco Hufnagel and Bernhard Klemt. I have always appreciated our pleasant and humorous conversations during our regular "Sauerbratenmontage" as a relaxing and enjoyable complement to my work.

Eidesstattliche Versicherung

Nocon, Madita Franziska
Name, Vorname

312834
Matrikelnummer (freiwillige Angabe)

Ich versichere hiermit an Eides Statt, dass ich die vorliegende Arbeit/Bachelorarbeit/ Masterarbeit* mit dem Titel

Discrete-Event Simulations of Quantum Random Walks, Quantum Key Distribution, and Related Experiments

selbständig und ohne unzulässige fremde Hilfe erbracht habe. Ich habe keine anderen als die angegebenen Quellen und Hilfsmittel benutzt. Für den Fall, dass die Arbeit zusätzlich auf einem Datenträger eingereicht wird, erkläre ich, dass die schriftliche und die elektronische Form vollständig übereinstimmen. Die Arbeit hat in gleicher oder ähnlicher Form noch keiner Prüfungsbehörde vorgelegen.

Aachen,
Ort, Datum

Unterschrift

*Nichtzutreffendes bitte streichen

Belehrung:

§ 156 StGB: Falsche Versicherung an Eides Statt

Wer vor einer zur Abnahme einer Versicherung an Eides Statt zuständigen Behörde eine solche Versicherung falsch abgibt oder unter Berufung auf eine solche Versicherung falsch aussagt, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

§ 161 StGB: Fahrlässiger Falscheid; fahrlässige falsche Versicherung an Eides Statt

(1) Wenn eine der in den §§ 154 bis 156 bezeichneten Handlungen aus Fahrlässigkeit begangen worden ist, so tritt Freiheitsstrafe bis zu einem Jahr oder Geldstrafe ein.

(2) Straflosigkeit tritt ein, wenn der Täter die falsche Angabe rechtzeitig berichtigt. Die Vorschriften des § 158 Abs. 2 und 3 gelten entsprechend.

Die vorstehende Belehrung habe ich zur Kenntnis genommen:

Aachen,
Ort, Datum

Unterschrift