Master of Science Thesis in Computer Science and Engineering
Department of Electrical Engineering, Linköping University, 2020

Active Phase Compensation in a Fiber-Optical Mach-Zehnder Interferometer

Joakim Argillander

Master of Science Thesis in Computer Science and Engineering

Active Phase Compensation in a Fiber-Optical Mach-Zehnder Interferometer

Joakim Argillander

LiTH-ISY-EX–20/5297–SE

Supervisor: **Alvaro Alarcón**
ISY, Linköping University

Examiner: **Guilherme B. Xavier**
ISY, Linköping University

Division of Information Coding
Department of Electrical Engineering
Linköping University
SE-581 83 Linköping, Sweden

Copyright © 2020 Joakim Argillander

Sammanfattning

Det här examensarbetet undersöker fenomenet fasstabilitet i en fiber-optisk MZI (*Mach-Zehnder-Interferometer*). MZI:n är en viktig byggsten i optiska system som används till experiment med både kontinuerligt emitterande lasrar och med enskilda fotoner. Genom att dela upp inkommande ljus i två strålar och låta det interferera med sig själv så bildas ett interferensmöster vid utgången vilket kan användas för att koda information. Det här är huvudprincipen bakom, till exempel, experiment inom QKD (*kvantnyckeldistribution, eng: Quantum Key Distribution*). Denna interferens förutsätter en koherens (högre än längdskillnaden mellan strålarna) mellan strålarna som det inkommande ljuset är uppdelat i. Särskilt måste fasen hos de bägge strålarna vara lika för att åstadkomma fullständig konstruktiv intereferens. Om en stråle är fasförskjuten (i förhållande till den andra) på grund av att ljuset har färdats en längre sträcka så uppnås endast delvis konstruktiv interferens. Om fasförskjutningen även varierar med tiden så leder det till ett system där experiment inte längre kan pålitligt utföras. Sådana fluktuationer är orsakade av termiskt-, akustiskt samt mekaniskt varierande effekter. Fiberoptiska interferometrar är särskilt känsliga mot förändringar i vågledarnas längd. Detta på grund av att det fiberoptiska mediet dras ihop respektive sträcks ut med temperaturen samt att fibern har en större ytarea som cirkulerande luft kan påverka mekaniskt jämfört med interferometrar konstruerade av bulkoptik.

I det här examensarbetet presenteras en lösning på problemet med miljöinducerad fasskift genom att utvärdera reglertekniska återkopplande algoritmer. Algoritmerna PID (*Proportionell-, Integrerande-, Deriverande regulator*) samt ICA (*Inkrementell Regleralgoritm, eng: Incremental Control Algorithm*) har undersökts och deras prestanda har jämförts med samt utan avskärmning. Algoritmerna har implementerats i en FPGA (*fältprogrammerbar grindmatris, eng: Field-Programmable Gate Array*) och regulatorn styr en elektrooptisk fasmodulator som kan addera en fasförskjutning till en av ljusstrålarna i MZI:n.

Resultat visar att passiv avskärmning inte är tillräckligt utan behöver användas tillsammans med aktiv reglering för att uppnå stabilitet över en längre tidsperiod. Detta examensarbete visar på att en signifikant förbättring i den optiska stabiliteten kan uppnås med aktiv reglering jämfört med en interferometer utan aktiv fasreglering.

Abstract

This thesis investigates the phenomena of phase stability in a fiber-optical MZI (*Mach-Zehnder Interferometer*). The MZI is a key building block of optical systems for use in experiments with both continuous-wave light and with single photons. By splitting incoming light into two beams and allowing it to interfere with itself an interference pattern is visible at the output, and this phenomena can be used to code information. This is the operating principle in, for example, QKD (*Quantum Key Distribution*) experiments. This interference requires coherence that is higher than the length difference between the beams that the incoming light is split into. Particularly the phase of the beams must be equal to achieve constructive interference. If one beam is phase-shifted (with respect to the other) due to the light having traversed a longer path, only partially constructive interference is achieved. If the phase shift also varies with time this leads to a system where experiments can no longer reliably be performed. Sources of these fluctuations are thermal, acoustic or mechanical. Fiber-optical interferometers are particularly sensitive to path length fluctuations of the waveguides as the fiber-optic medium contracts and elongates with temperature, and also has a larger surface area for circulating air to mechanically disturb the waveguides than bulk optics interferometers.

In this thesis, a solution to environment-induced phase drift is presented by evaluating implementations of feedback algorithms for automatic control. The algorithms PID (*Proportional-, Integral-, Derivative controller*) and an ICA (*Incremental Control Algorithm*) have been investigated and the performance of these controllers has been compared when used with, and without, optical enclosures. The algorithms are implemented in an FPGA (Field-Programmable Gate Array) and the controller actuates an electro-optical phase modulator that can add a phase shift to one of the light beams in the MZI. This thesis shows that significant improvement in the optical stability can be achieved with active control compared to an interferometer without active phase control.

Acknowledgments

I would like to thank Dr. Guilherme B. Xavier for being my examiner and for the opportunity to do my master's thesis in collaboration with the Information Coding Group. Thanks for introducing me to the area of quantum information.

I would also like to thank my supervisor, Alvaro Alarcón for valuable discussions and ideas. A special thanks for all the help in the lab with the optics equipment and for helping out with theory.

Linköping, June 2020
Joakim Argillander

Contents

Notation **xi**

1 Introduction **1**
1.1 Background and Purpose 1
1.2 Problem Statement 2
1.3 Related Work 2
1.4 Delimitations 3

2 Theory **5**
2.1 One-Time Pad 5
2.2 Quantum Key Distribution 5
2.2.1 Bennett-Brassard 1984 6
2.2.2 Security of Quantum Key Distribution 12
2.3 Encoding Information in Quantum States 15
2.3.1 Polarization Coding 15
2.3.2 Phase Coding 16
2.4 Interferometric Generation of Quantum States 17
2.4.1 Mach-Zehnder Interferometer 17
2.4.2 Interference in a Mach-Zehnder Interferometer 19
2.4.3 Interferometric Visibility and Distinguishability 21
2.5 Few-Mode Mach-Zehnder Interferometer 23

3 Method **27**
3.1 Experiment Setup 27
3.1.1 Fiber-Optical Mach-Zehnder Interferometer 27
3.1.2 Alignment of Mach-Zehnder Interferometer 27
3.1.3 Optical Enclosure 28
3.1.4 Background Drift Characterization 28
3.1.5 Control Circuitry 28
3.2 Performance Metrics 29
3.2.1 Mean-Squared Error 30
3.2.2 Standard Deviation 30
3.2.3 Performance Metric Discussion 30

3.3 Control Algorithms 30
3.3.1 Feedback Control 31
3.3.2 Incremental Control Algorithm 32
3.3.3 PID-Controller 33
3.4 FPGA-circuit 36
3.4.1 ADC-/DAC-block 36
3.4.2 Controller block 36

4 Results and Discussion 39
4.1 Stand-Alone MZI 39
4.1.1 Phase Drift Without Control 39
4.1.2 Stand-Alone MZI with PID-controller 41
4.1.3 Stand-Alone MZI with ICA-controller 44
4.2 Few-Mode MZI 46
4.2.1 Background Drift Uncontrolled 47
4.2.2 Few-Mode MZI with PID-controller 48
4.3 Quantitative Comparison 50
4.3.1 Mean Squared-Error 50
4.3.2 Standard deviation 50
4.3.3 Setpoint 51
4.4 General Discussion 52

5 Conclusions 53
5.1 Future Work 53

A FPGA Block Diagrams 57

B Photograph: Control Electronics 59

C Photograph: Interferometer Setup 61

Bibliography 65

Notation

Notation

Notation	Description
i	Imaginary unit $i^2 = -1$
$A^\dagger$	Hermitian conjugate of vector A
$\langle\phi\|$	Bra-vector describing the linear functional ϕ
$\|\psi\rangle$	Ket-vector describing the quantum state ψ
$\mathbb{N}$	The set of natural numbers
$\mathbb{Z}$	The set of integers
$\|\vec{u}\|$	Vector norm of vector $\vec{u}$
$\vec{u} \bullet \vec{v}$	Scalar product of $\vec{u}$ and $\vec{v}$
$\mathrm{Pr}(\mathrm{X}\|\mathrm{Y})$	Conditional probability of X given Y
$\mathrm{proj}_{\vec{v}}(\vec{u})$	Orthogonal projection of vector $\vec{u}$ onto vector $\vec{v}$

Abbreviations

Abbreviation	Description
ADC	Analog-to-Digital Converter
BB84	Bennett-Brassard 1984
DAC	Digital-to-Analog Converter
DSO	Digital Storage Oscilloscope
FM	Few-Mode
FMF	Few-Mode Fiber
FPGA	Field-Programmable Gate Array
ICA	Incremental Control Algorithm
MSE	Mean-Squared Error
MZI	Mach-Zehnder Interferometer
PM	Phase Modulator
PL	Photonic Lantern
PC	Polarization Controller
PID	Proportional-, Integral-, Derivative (controller)
QKD	Quantum Key Distribution
QBER	Quantum Bit-Error Rate
SA	Standalone
SD	Standard Deviation
SM	Single-Mode
VHDL	Very High Speed Integrated-Circuit Hardware Description Language
WDM	Wavelength-Division Multiplexing

1 Introduction

This thesis will investigate methods for *phase-stabilization* or *phase-correction* in fiber-optical interferometric quantum key distribution systems. The term *active* in this thesis refers to the continuous on-line compensation for phase drift while the system is in operation.

1.1 Background and Purpose

The art of protecting information that is transmitted over public channels is not a new concept. What has changed is the methods with which information is encrypted [1]. Harnessing elementary particles allows for encryption schemes where total security can be achieved. Most commonly, photons are used as bearer of information over a quantum channel which thus requires an optoelectrical system for the transmission and encoding of data. Many systems generating the quantum states that are required for quantum key distribution are based on interference phenomena in optical interferometers [2].

The interferometer, while being a versatile optical tool for instrumentation, is intrinsically exceptionally sensitive to environmental noise [3]. Sources of noise include high frequency noise stemming from vibrations [3], but also low-frequency noise due to thermal fluctuations leading to elongation and contraction of the fiber-optic cables. Quantum experiments are mostly performed on dampened optical tables that act as low-pass filters by isolating the experimental setup from the ground. However, this is not an effective filter against low-frequency noise from the environment.

Although passively damping enclosures exist that are able to eliminate disturbances from moving air, a solution is required to eliminate the impact of any

residual phase instability. In order to reliably generate distinguishable quantum states so that low quantum bit error rate (QBER) communication can be carried out, the interferometer has to be stabilized from such fluctuations.

1.2 Problem Statement

The aim of this thesis is to address the following questions

- How can Field-Programmable Gate Array's (FPGA) be used to control phase modulation of a Mach-Zehnder interferometer (MZI)?
- How well does a phase stabilization system using an FPGA perform in a noisy environment?
- How well does a phase stabilization system work with an interferometer using spatial division multiplexing?
- What is the impact of optical enclosures on interferometers using active phase stabilization with regards to mean squared-error and standard deviation?

1.3 Related Work

Previous research in stabilization of interferometers is not limited to only consider Mach-Zehnder interferometers. Lu et al. propose an algorithm where an inlined phase modulator in a Faraday-Michelson interferometer arm is actuated with an applied voltage while the optical intensity is measured. The applied voltage is swept between voltages corresponding to one period of added phase. The phase modulator voltage that corresponds to the maximum intensity is applied as an offset to the voltages corresponding to the phase shifts in which information is coded. This forms a coding matrix that is valid for some coherence time, after which the process of scanning the channel is repeated to construct a new coding matrix [4].

Phase stabilization systems for single-photon interference using feedback loops have been investigated by Xavier and von der Weid where a PID-controller was used to phase lock a Mach-Zehnder interferometer. Two optical channels were multiplexed onto one fiber so that one could be used for phase coding and one in the feedback loop for the stabilization. The interferometer was subject to environmental noise of frequencies on the order of 100 Hz and a net visibility of 97% was achieved [5] with single-photons generated by attenuating a distributed feedback laser [5].

PID-control has also been researched by Seok-Beom and Tae-Gon where a Michelson interferometer was stabilized to achieve a phase error of only 0.06 rad yielding a net visibility of over 98% [6]. Both of these previous experiments have been done on long interferometers ($\geq$ 1 km). Both of the previous experiments have

been locking the phase in quadrature with a setpoint voltage V_{set} corresponding to a phase shift $\varphi = \pi/2$ [5, 6], thus operating in the linear region.

By considering a Mach-Zehnder interferometer as a tunable electrooptical modulator, Ma et al. have shown that by stabilizing a MZI using an auxiliary HeNe counter-propagating beam it is possible to achieve a 88.7% ± 3.8% visiblity for Hong-Ou-Mandel two-photon interference [7]. The advantage of using a MZI as modulator is that the MZI is polarization-independent [7]. Polarization is a desirable and convenient degree of freedom for encoding information and enables a Mach-Zehnder modulator to be used as a building block for quantum gates [7].

1.4 Delimitations

This thesis will only consider a fiber-optic Mach-Zehnder interferometer with a laser source operating in the C-band (1530 – 1565 nanometer). The laser will be considered wavelength-stable around its central wavelength. Further, the experiment setup will be limited to telecommunications-grade optics over single-mode fibers. All optical components are selected such that the wavelength of the laser source is within the component's operating wavelength range.

The output of the photodetector is limited to a bandwidth of 1 kHz, and thus the FPGA-circuit, the analog-to-digital converter (ADC) and digital-to-analog converter (DAC) is also only designed to operate within that range. The driving circuit will be limited to the bandwidth of the photodetector and will thus be assembled on a breadboard.

Data acquisition will be done with a digital storage oscilloscope (DSO) limited to a bandwidth of 70 MHz, 2 GS/s and a capacity of recording a maximum experiment length of 1500 seconds.

2 Theory

In this chapter the theory behind quantum key distribution is presented, as well as theory for interferometric generation of the quantum states required for communication over a quantum channel.

2.1 One-Time Pad

The one-time pad is a cryptographically secure encryption scheme that relies on pre-shared keys to achieve secrecy. Given that both the sender and the recipient in a symmetric encryption scheme have a pre-shared key (of length equal to the message to be encrypted) that has been generated through a truly random process, and is only used once, unconditional secrecy can be achieved [8, 9]. However, the issue with one-time pads is related to how the keys are initially shared.

The ability of QKD to generate keys where secret data bits never pass over an unsecured channel makes it suitable for use together with one-time pad encryption schemes [9].

2.2 Quantum Key Distribution

Quantum key distribution is a provably secure method for parties to generate a shared key. Quantum key distribution is illustrated using the BB84-protocol. However, other protocols exist that all utilize fundamental quantum properties to encode so-called quantum bits, qubits.

2.2.1 Bennett-Brassard 1984

Bennet and Brassard first proposed the BB84-protocol [10] in 1984. The protocol is based on the quantum principle that information cannot be be gained without also destroying the signal and that qubits cannot be cloned [11].

The key distribution process is illustrated between two parties, Alice and Bob with an eavesdropper, Eve who wants to obtain information about the key. The protocol is illustrated in two dimensions.

General Bases

The quantum state ψ can be written as a linear combination (*ket*-vector) of the preparation bases like

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{2.1}$$

for some orthogonal basis vectors

$$\begin{aligned} |0\rangle &= \begin{pmatrix} x_1 & y_1 \end{pmatrix}^{\mathbf{T}} \\ |1\rangle &= \begin{pmatrix} x_2 & y_2 \end{pmatrix}^{\mathbf{T}} \end{aligned} \tag{2.2}$$

such that $|0\rangle \perp |1\rangle$ and complex probability amplitudes α respectively β that obey the normalization

$$|\alpha|^2 + |\beta|^2 = 1 \tag{2.3}$$

such that the total probability is equal to 1. The dual of the ket (the *bra*-vector) is the Hermitian conjugate of the ket, and is defined

$$\begin{aligned} \langle\psi| &= |\psi\rangle^{\dagger} \\ &= \Big(\alpha|0\rangle + \beta|1\rangle\Big)^{\dagger} \\ &= \alpha^*\langle 0| + \beta^*\langle 1| \end{aligned} \tag{2.4}$$

where α^* respectively β^* denote the complex conjugate of α and β.

Measurement of Quantum States

Measurement of a quantum state ψ is dependent on a measurement basis

$$|\phi\rangle = \gamma|0\rangle + \delta|1\rangle \tag{2.5}$$

and measurement of a qubit is seen as the probability amplitude[1] for the state ψ to collapse into the state ϕ. This is calculated mathematically as the orthogonal projection of ψ onto ϕ and is denoted $\langle\phi|\psi\rangle$.

The orthogonal projection of ψ onto ϕ is the scalar product

$$\begin{aligned}
\langle\phi|\psi\rangle &= |\phi\rangle^{\dagger}|\psi\rangle \\
&= \Big(\gamma|0\rangle + \delta|1\rangle\Big)^{\dagger} \bullet \Big(\alpha|0\rangle + \beta|1\rangle\Big) \\
&= \Big(\gamma^{*}\langle 0| + \delta^{*}\langle 1|\Big)^{\dagger} \bullet \Big(\alpha|0\rangle + \beta|1\rangle\Big) \\
&= \alpha\gamma^{*}\underbrace{\langle 0|0\rangle}_{=1} + \beta\gamma^{*}\underbrace{\langle 0|1\rangle}_{=0} + \alpha\delta^{*}\underbrace{\langle 1|0\rangle}_{=0} + \beta\delta^{*}\underbrace{\langle 1|1\rangle}_{=1} \\
&= \alpha\gamma^{*} + \beta\delta^{*}
\end{aligned} \tag{2.6}$$

where † denotes the Hermitian conjugate as derived in Equation 2.4.

Orthogonal projection is idempotent [12] such that $\text{proj}_{\vec{v}}(\vec{v}) = \vec{v}$ from which it follows that $\langle 0|0\rangle = \langle 1|1\rangle = 1$. Also $\text{proj}_{\vec{u}}(\vec{v}) = \vec{0}$ if $\vec{v} \perp \vec{u}$ from which it follows that $\langle 0|1\rangle = \langle 1|0\rangle = 0$.

Probability of Measurements

The probability for ψ to collapse into ϕ is obtained from Equation2.6 through

$$\Big|\langle\phi|\psi\rangle\Big|^{2} = \Big|\alpha\gamma^{*} + \beta\delta^{*}\Big|^{2}. \tag{2.7}$$

In other words, Equation 2.7 describes the probability that the transmitted qubit $|\psi\rangle$ is correctly[2] measured given that it is measured in the basis ϕ.

Preparation of Quantum States

Let ψ_{ij} denote the qubit ψ that has encoded a binary digit j in the basis i. Then two preparation bases ψ_{0j} and ψ_{1j} can be formed as

$$\begin{aligned}
|\psi_{00}\rangle &= |0\rangle \\
|\psi_{01}\rangle &= |1\rangle \\
|\psi_{10}\rangle &= \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \\
|\psi_{11}\rangle &= \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle
\end{aligned} \tag{2.8}$$

[1] This is a complex quantity and is separate from classical probability

[2] *Correct* in this case means to unambiguously decode the qubit into the transmitted state

and the qubits are no longer distinguishable as the mutual orthogonality is lost.

Two-dimensional quantum states have three mutually orthogonal basis sets. By applying a phase shift of $\pm\frac{\pi}{2}$ a third can be constructed from

$$\begin{aligned} |\psi_{x0}\rangle &= \frac{1}{\sqrt{2}}|0\rangle + i\frac{1}{\sqrt{2}}|1\rangle \\ |\psi_{x1}\rangle &= \frac{1}{\sqrt{2}}|0\rangle - i\frac{1}{\sqrt{2}}|1\rangle \end{aligned} \tag{2.9}$$

by multiplication with $\pm i$. Of course, since these three bases together span a three-dimensional space, but (binary) data is encoded in two dimensions, only two bases are selected to encode the data. In fact, any two of these bases can be used.

Given any two such bases, for example ψ_{0j} and ψ_{1j}, two participants of a key exchange, Alice and Bob can generate a provably secure key for further use with conventional symmetric encryption algorithms [13]. The protocol only assumes that Alice and Bob have access to one quantum channel and one authenticated classical channel [2]. Neither of these channels need to be secure in a traditional sense, other than that both channels need to be unjammable.

Transmission of Quantum Bits

Alice generates a truly random string of bits of length n called the *basis selection*. This string is used to select which basis to encode information in the qubit in. She also generates another random string, also of length n which is the data bits that she will send to Bob. These bits are encoded into qubits bitwise by encoding bit k in the data string using the basis determined by bit k in the basis selection. For example, if Alice has generated the following data bits and basis selection

Data bits:	0111001101...
Basis selection:	1011010001...

this yields the following string of qubits

$$|\psi_{10}\rangle \quad |\psi_{01}\rangle \quad |\psi_{11}\rangle \quad |\psi_{11}\rangle \quad |\psi_{00}\rangle \quad |\psi_{10}\rangle \quad |\psi_{01}\rangle \quad |\psi_{01}\rangle \quad |\psi_{00}\rangle \quad |\psi_{11}\rangle$$

that she subsequently transmits over a quantum channel.

Reception of Quantum Bits

Before beginning to receive qubits over the quantum channel, Bob also generates a truly random basis selection. This dictates what bases Bob will be using to measure the received qubit.

k	Basis	Received bit	Measurement	
1	ϕ_{0j}	**R**	$\langle\phi_{0j}\|\psi_{10}\rangle$	
2	ϕ_{0j}	1	$\langle\phi_{0j}\|\psi_{01}\rangle$	
3	ϕ_{1j}	1	$\langle\phi_{1j}\|\psi_{11}\rangle$	
4	ϕ_{1j}	1	$\langle\phi_{1j}\|\psi_{11}\rangle$	
5	ϕ_{1j}	**R**	$\langle\phi_{1j}\|\psi_{00}\rangle$	
6	ϕ_{1j}	0	$\langle\phi_{1j}\|\psi_{10}\rangle$	
7	ϕ_{0j}	1	$\langle\phi_{0j}\|\psi_{01}\rangle$	
8	ϕ_{1j}	**R**	$\langle\phi_{1j}\|\psi_{01}\rangle$	
9	ϕ_{0j}	1	$\langle\phi_{0j}\|\psi_{00}\rangle$	ϵ
10	ϕ_{0j}	**R**	$\langle\phi_{0j}\|\psi_{11}\rangle$	
$\vdots$	$\vdots$	$\vdots$	$\vdots$	

Table 2.1: *Bob's received data bits and the quantum measurements done.* ***R*** *(for random) signifies received qubits where Bob measures in the wrong basis and thus has a 50% probability to obtain precisely the bit value that Alice sent.* ϵ *denotes a bit that was erroneously decoded.*

Let ϕ_{0j} and ϕ_{1j} denote Bob's orthogonal bases in which he will measure the received qubits, defined like Alice's preparation bases in Equation 2.8. Note that, out of the set of three possible bases, Alice and Bob must use the same two bases throughout the transmission. Then he can form a selection of bases in which to measure the received qubit. For example, if Bob has generated the following basis selection

$$\text{Basis selection:} \qquad 0011110100\ldots$$

his measurement bases, in sequence, will be

$$\langle\phi_{0j}| \quad \langle\phi_{0j}| \quad \langle\phi_{1j}| \quad \langle\phi_{1j}| \quad \langle\phi_{1j}| \quad \langle\phi_{1j}| \quad \langle\phi_{1j}| \quad \langle\phi_{1j}| \quad \langle\phi_{1j}| \quad \langle\phi_{1j}|$$

and by receiving qubits and measuring them he obtains the results in Table 2.1. Indeed there is no way for Bob to know whether he has measured the received qubit correctly and obtained the data bit that was sent by Alice. The probability that Bob's measurement yielded the bit that Alice encoded and sent is shown in Table 2.2 and it shows that in the cases where Bob's choice of measurement basis does not coincide with Alice's, there is a 50% probability that Bob's measurement was correct and that measurement does not contain any useful information. Hence, the received key must be sifted.

k	Measurement	Probability amplitude	Probability
1	$\langle\phi_{0j}\|\psi_{10}\rangle$	$\frac{1}{\sqrt{2}}$	$\frac{1}{2}$
2	$\langle\phi_{0j}\|\psi_{01}\rangle$	1	1
3	$\langle\phi_{1j}\|\psi_{11}\rangle$	1	1
4	$\langle\phi_{1j}\|\psi_{11}\rangle$	1	1
5	$\langle\phi_{1j}\|\psi_{00}\rangle$	$\frac{1}{\sqrt{2}}$	$\frac{1}{2}$
6	$\langle\phi_{1j}\|\psi_{10}\rangle$	1	1
7	$\langle\phi_{0j}\|\psi_{01}\rangle$	1	1
8	$\langle\phi_{1j}\|\psi_{01}\rangle$	$\frac{1}{\sqrt{2}}$	$\frac{1}{2}$
9	$\langle\phi_{0j}\|\psi_{00}\rangle$	1	1
10	$\langle\phi_{0j}\|\psi_{11}\rangle$	$\frac{1}{\sqrt{2}}$	$\frac{1}{2}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$

Table 2.2: *Probability that Bob's measurement yielded the bit that was sent by Alice.*

Sifting

In order to distill a usable key from the unsifted key that was received by Bob, Alice and Bob communicate their choices of bases and discard the bits where Alice's choice does not match Bob's. Table 2.3 shows the sifting process. After one pass through the key, both parties now share a correlated key of equal length. While the key is highly correlated, it is not identical and cannot be used for encryption yet.

Revealing the basis choices does not reveal any information about the final key. Due to the intrinsic lack of information about the final key in the communication of the parties' basis choices, this communication can be performed over a non-secured channel [2].

Due to the random selection of measurement bases, approximately $n/2$ bits of the unsifted key remain after the sifting process [2].

k	Received bit	Measurement
$\cancel{1}$	$\cancel{\mathbf{R}}$	$\cancel{\langle\phi_{0j}\|\psi_{10}\rangle}$
2	1	$\langle\phi_{0j}\|\psi_{01}\rangle$
3	1	$\langle\phi_{1j}\|\psi_{11}\rangle$
4	1	$\langle\phi_{1j}\|\psi_{11}\rangle$
$\cancel{5}$	$\cancel{\mathbf{R}}$	$\cancel{\langle\phi_{1j}\|\psi_{00}\rangle}$
6	0	$\langle\phi_{1j}\|\psi_{10}\rangle$
7	1	$\langle\phi_{0j}\|\psi_{01}\rangle$
$\cancel{8}$	$\cancel{\mathbf{R}}$	$\cancel{\langle\phi_{1j}\|\psi_{01}\rangle}$
9	1	$\langle\phi_{0j}\|\psi_{00}\rangle$
$\cancel{10}$	$\cancel{\mathbf{R}}$	$\cancel{\langle\phi_{0j}\|\psi_{11}\rangle}$
$\vdots$	$\vdots$	$\vdots$ $\vdots$

Table 2.3: *Sifting of the received key. Both Alice and Bob discard bits where their choices of basis does not match. The circled bit shows where Bob has obtained the value 1, using the correct basis while Alice sent a 0. That is, a bit error has occurred as a consequence of either transmission errors or from an eavesdropper.*

Alice:		
	Sifted key:	111010...
Bob:		
	Sifted key:	111010...

Table 2.4: *Sifted key containing bit errors.*

Information Reconciliation and Privacy Amplification

The sifted key in Table 2.4 still contains errors. These errors may stem from transmission errors or from an eavesdropper on the channel. Thus, a step called *information reconciliation* and *privacy amplification* must be performed.

Again, Alice and Bob communicate over the public channel and compare the value of a chosen bit in the sifted key. Bit m in Bob's sifted key is compared to bit m in Alice's data bits. This consumes the bit and both parties discard that from

the final generated key, taking note of whether the bits are equal or not. This way, both erroneous bits and bits that were correct are discarded.

The error is expressed as

$$\varepsilon = \frac{\text{number of erroneous bits}}{\text{total number of bits}}. \tag{2.10}$$

Alice and Bob perform information reconciliation in Table 2.5 by probing bit 3 and 6 thus discarding them, noting that Bob's bit 6 does not match Alice's. Whether this is due to transmission errors or due to an eavesdropper cannot be determined from one bit alone. The error in this case is $\varepsilon = 1/4 = 25\%$.

Alice:		
	Sifted key:	$11\underset{\uparrow}{\cancel{1}}01\underset{\uparrow}{\cancel{1}}\ldots$
Bob:		
	Sifted key:	$11\underset{\uparrow}{\cancel{1}}01\underset{\uparrow}{\cancel{0}}\ldots$
Alice:		
	Final key:	$1101\ldots$
Bob:		
	Final key:	$1101\ldots$

Table 2.5: *Privacy amplification by probing and discarding probed bits*

The probability P_D that an eavesdropper is detected by probing and discarding n bits is given by

$$P_D = 1 - \left(\frac{3}{4}\right)^n. \tag{2.11}$$

and therefore, the probability to detect an eavesdropper can be made arbitrarily high by choosing n sufficiently large.

2.2.2 Security of Quantum Key Distribution

The following section illustrates how an eavesdropper is detected in a Bennett-Brassard protocol key exchange.

Eavesdropping through Interception and Resending

An eavesdropper that intercepts the quantum channel is not able to measure the qubit without also destroying it and it is desirable for an eavesdropper to listen to a channel without being noticed. Eavesdropping on a quantum channel therefore

entails intercepting the qubit and measuring it before re-preparing it and sending it to the original recipient.

An eavesdropper, Eve, without knowledge of Alice's preparation bases must also select a measurement basis ϕ'_{ij}. Since Alice's choice is truly random, there exists no information from which a future basis choice can be predicted. Hence, Eve can, at best, choose her measurement bases at random [14]. Then Eve has 50% chance to measure the qubit in the same basis as it was encoded and obtain the correct encoded data. Eve has to resend the qubit to Bob, and does so by preparing a qubit using the same basis as she measured in. It would be unreasonable to prepare the state in a different basis than what she measured, as the error would then always be 25%.

If Eve's measurement basis is wrong[3], then the probability for her to measure the correct data bit is 50%, and then sending a qubit in the same basis yields a probability of 50% for Bob to measure the data bit that Alice originally sent. Thus in the presence of Eve, Bob has a $50\% \cdot 50\% = 25\%$ probability to measure the data bit which was originally encoded by Alice.

Thus, the quantum bit error rate $\varepsilon \rightarrow 0.25$ in the presence of an eavesdropper [2, 14].

Table 2.6 shows the probabilities of correct measurements for each party in the exchange of one qubit. The quantity $\left|\langle x|y\rangle\right|^2$ shows the probability that the measurement is correct with respect to the previous preparation, and $\Pr(M|A)$ the probability that the measured state M is the state A which Alice initially sent.

As such, quantum key distribution does not distribute a pre-generated key but rather, the cryptographically secure key is generated as part of the process. In other words, the goal is not data transfer from Alice to Bob, but to generate two keys, one at Alice and one at Bob which are both highly correlated.

[3] With respect to Alice's preparation basis

	ALICE			EVE			BOB
	P		M		P		M
State:	$\lvert\psi_{ij}\rangle$	$\longrightarrow$	$\langle\phi'_{ij}\rvert$	$\rightharpoonup$	$\lvert\phi'_{ij}\rangle$	$\longrightarrow$	$\langle\phi_{ij}\rvert$
State:	$\lvert\psi_{10}\rangle$	$\longrightarrow$	$\langle\phi'_{01}\rvert$	$\rightharpoonup$	$\lvert\phi'_{01}\rangle$	$\longrightarrow$	$\langle\phi_{11}\rvert$
Data:	0		1		1		1
$\left\lvert\langle x\rvert y\rangle\right\rvert^2$			$\frac{1}{2}$				$\frac{1}{2}$
$\Pr(M\rvert A)$			$\frac{1}{2}$				$\frac{1}{4}$

Table 2.6: *Bit errors induced by eavesdropping at the time of measuring (M) respectively preparing (P) the qubit.*

2.3 Encoding Information in Quantum States

Information bits have to be coded in qubits in order to utilize the quantum mechanical effects that ensure security. The two most common encoding schemes are polarization coding and phase coding, but any two orthogonal states can be used to form bases. In each of the bases, one basis vector is chosen to represent a binary one and the other vector represents a binary zero.

The BB84 protocol is independent of what physical phenomena is used to encode qubits. Many different coding schemes exist, where polarization coding and phase coding are two of them.

2.3.1 Polarization Coding

Traditional quantum key distribution schemes such as the algorithm proposed by Bennet and Brassard encode the data bits in the linear polarization of the transmitted photons [10]. Orthogonal angles of polarization form basis vectors in which the information is coded.

In practical implementations the two measurement bases are traditionally the so-called *horizontal* base with basis vectors 0° and 90°, and the *diagonal* basis with basis vectors ±45°. Thus, one of the valid encodings can be expressed using notation from Equation 2.8 as

$$\begin{aligned}
|\psi_{00}\rangle &= |0^\circ\rangle \\
|\psi_{01}\rangle &= |90^\circ\rangle \\
|\psi_{10}\rangle &= \frac{1}{\sqrt{2}}|0^\circ\rangle + \frac{1}{\sqrt{2}}|90^\circ\rangle = \\
&= |45^\circ\rangle \\
|\psi_{11}\rangle &= \frac{1}{\sqrt{2}}|0^\circ\rangle - \frac{1}{\sqrt{2}}|90^\circ\rangle = \\
&= |-45^\circ\rangle
\end{aligned} \tag{2.12}$$

and, for completeness, the remaining third basis that is given by Equation 2.9 corresponds to circular polarization through

$$\begin{aligned}
|\psi_{x0}\rangle &= \frac{1}{\sqrt{2}}|0^\circ\rangle + i\frac{1}{\sqrt{2}}|90^\circ\rangle = \\
&= |\circlearrowleft\rangle \\
|\psi_{x1}\rangle &= \frac{1}{\sqrt{2}}|0^\circ\rangle - i\frac{1}{\sqrt{2}}|90^\circ\rangle = \\
&= |\circlearrowright\rangle.
\end{aligned} \tag{2.13}$$

Polarization coding is commonly used in experimental setups based on free-space optical quantum channels due to the retention of polarization reference frames

through the entire transmission path.

2.3.2 Phase Coding

Due to intrinsic time-dependent birefringence effects in optical fibers that may render one polarization state indistinguishable from another [2, 14], a more robust scheme must be employed. If one quantum state cannot be distinguished from others reliably, then the quantum bit-error rate QBER increases. It follows then that the certainty with which an eavesdropper can be detected is lowered.

Phase coding encodes the information bits in the phase angle of photons from a laser source. Phase coding does not suffer from birefringence artifacts and is thus a suitable alternative for fiber-optical QKD. Following the indexing convention in Equation 2.8, a valid phase coding scheme is given by Equation 2.14. Note that orthogonality in phase coding schemes is achieved for basis vectors with a phase angle of π between them instead of $\pi/2$ as with polarization coding.

$$
\begin{aligned}
|\psi_{00}\rangle &= |U\rangle \\
|\psi_{01}\rangle &= |L\rangle \\
|\psi_{10}\rangle &= \frac{1}{\sqrt{2}}\left(|U\rangle + |L\rangle\right) \\
|\psi_{11}\rangle &= \frac{1}{\sqrt{2}}\left(|U\rangle - |L\rangle\right) \\
|\psi_{x0}\rangle &= \frac{1}{\sqrt{2}}\left(|U\rangle + i|L\rangle\right) \\
|\psi_{x1}\rangle &= \frac{1}{\sqrt{2}}\left(|U\rangle - i|L\rangle\right)
\end{aligned}
\tag{2.14}
$$

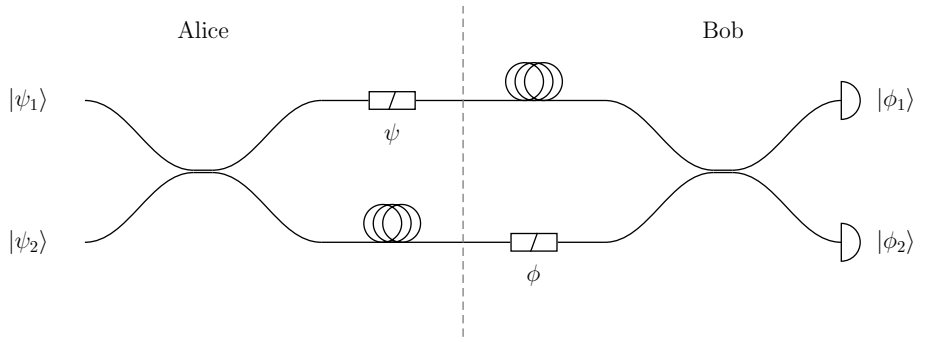


Figure 2.1: *Quantum key distribution using phase coding.*

Figure 2.1 shows a a Mach-Zehnder interferometer setup for QKD using phase encoded qubits. To encode a qubit, Alice selects a preparation basis using the phase modulator ψ and Bob selects measurement basis using the phase modulator ϕ.

Alice sends a binary one in basis ψ by sending a photon in the upper arm and a binary zero by sending a photon in the lower arm. If Bob's phase equals Alice's, then he will also detect a photon in the upper arm.

2.4 Interferometric Generation of Quantum States

The interferometer is a versatile apparatus for experiments in the optical domain. Young's double slit experiment initially showed wave interference of light in 1801, and the fundamental principle of interference between superimposed electromagnetic waves is still the main operating principle behind interferometers.

2.4.1 Mach-Zehnder Interferometer

The Mach-Zehnder interferometer measures the relative phase shift between two beams of light as shown in Figure 2.2. Light enters a beamsplitter (BS1) that splits the beam into two beams of equal intensity. The two beams are called the upper and the lower arms of the interferometer respectively. Both arms have inline polarization controllers (PC1 and PC2) with which the polarization of the light can be controlled. The upper arm has an additional electro-optical phase modulator (PM) which can add a phase shift to the light beam traversing the upper arm. Both arms are terminated in a recombining beamsplitter (BS2). Since the light beams are highly coherent they will interfere, and an interference pattern is visible at either detector (Detector 1 or Detector 2).

The interference pattern depends on the relative phase difference between the arms. The interference pattern as a function of the phase difference is derived in Chapter 2.4.2.

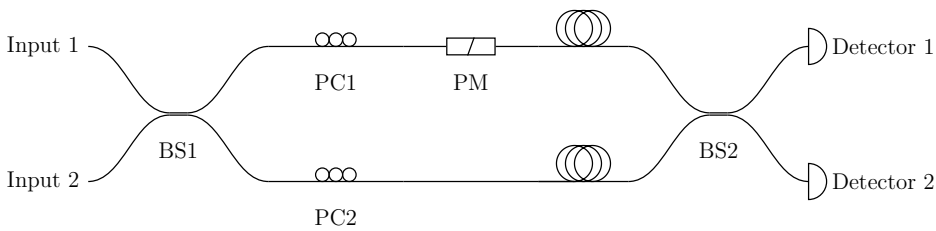


Figure 2.2: *Mach-Zehnder Interferometer (fiber-optic).*

Constant Phase Shift

Let l_u and l_l denote the optical path length of the upper and the lower arm and λ the wavelength of the optical source. The optical path is the path the light travels, which includes the length through beam splitters and phase controllers. This takes refractive indices and angle of incidence into account, and the optical

path may be longer than the physical path. The lower arm is then subject to a phase shift of

$$\varphi_{\mathrm{l}} = \frac{2\pi n l_{\mathrm{l}}}{\lambda} = 2\pi n \left(\frac{l_{\mathrm{l}}}{\lambda} \right) \tag{2.15}$$

while the upper arm is subject to a phase shift of

$$\varphi_{\mathrm{u}} = \frac{2\pi n l_{\mathrm{u}}}{\lambda} + \frac{2\pi n l_{\mathrm{pm}}(V)}{\lambda} = 2\pi n \left(\frac{l_{\mathrm{u}} + l_{\mathrm{pm}}(V)}{\lambda} \right) \tag{2.16}$$

for $n \in \mathbb{Z}$, due to the additional phase modulator inlined in the optical path, yielding an additional optical path length of l_{pm} as a function of an applied voltage V.

Then the relative phase shift is given by

$$\begin{aligned} \varphi &= \left| \varphi_{\mathrm{u}} - \varphi_{\mathrm{l}} \right| \\ &= \left| 2\pi n \left(\frac{l_{\mathrm{u}} + l_{\mathrm{pm}}(V)}{\lambda} \right) - 2\pi n \left(\frac{l_{\mathrm{l}}}{\lambda} \right) \right| \\ &= 2\pi n \left| \frac{l_{\mathrm{u}} + l_{\mathrm{pm}}(V) - l_{\mathrm{l}}}{\lambda} \right| \end{aligned} \tag{2.17}$$

and in the case of a balanced interferometer with equally long optical paths in the upper and lower arms, i.e. $l_{\mathrm{u}} = l_{\mathrm{l}}$ the phase shift is given by

$$\varphi = 2\pi n \left| \frac{l_{\mathrm{pm}}(V)}{\lambda} \right| \tag{2.18}$$

Time-varying Phase Shift

Equation 2.18 assumes that the interferometer is not subject to disturbances that affect the length of the arms, or that any such noise is uniformly affecting both arms so that any change in optical path length occurs at the same time in both. In practice, both l_{u} and l_{l} are not constant, but time-varying so the phase shift as a function of time can be written as

$$\begin{aligned} \varphi(t) &= \left| 2\pi n \left(\frac{l_{\mathrm{u}}(t) + l_{\mathrm{pm}}(V)}{\lambda} \right) - 2\pi n \left(\frac{l_{\mathrm{l}}(t)}{\lambda} \right) \right| \\ &= 2\pi n \left| \frac{l_{\mathrm{u}}(t) + l_{\mathrm{pm}}(V) - l_{\mathrm{l}}(t)}{\lambda} \right| \\ &= \frac{2n\pi}{\lambda} \left| \left[l_{\mathrm{u}}(t) - l_{\mathrm{l}}(t) \right] + l_{\mathrm{pm}}(V) \right| \end{aligned} \tag{2.19}$$

where $l_u(t)$ and $l_l(t)$ are the optical path length of the upper and lower arm as a function of time, respectively. By applying a voltage as a function of time, $V(t)$ to the phase modulator such that $\varphi(t) = \varphi_0$, the relative phase shift can be maintained constant. That is, locked to a constant phase difference of φ_0.

2.4.2 Interference in a Mach-Zehnder Interferometer

The wave function describes the probability amplitude that a single photon emerges at one of the outputs and is identical for both free-space configurations and fiber-optical configurations. Given equivalent components, neither the geometry of the paths nor the waveguides impact the resulting wave function. The state ψ_1 and ψ_2 correspond to the upper and lower inputs of the fiber-optic MZI in Figure 2.1, and b/b' and a the upper and lower arms in the same figure.

The derivation for the wave function for a general Mach-Zehnder interferometer is therefore illustrated in a free-space configuration as shown in Figure 2.3.

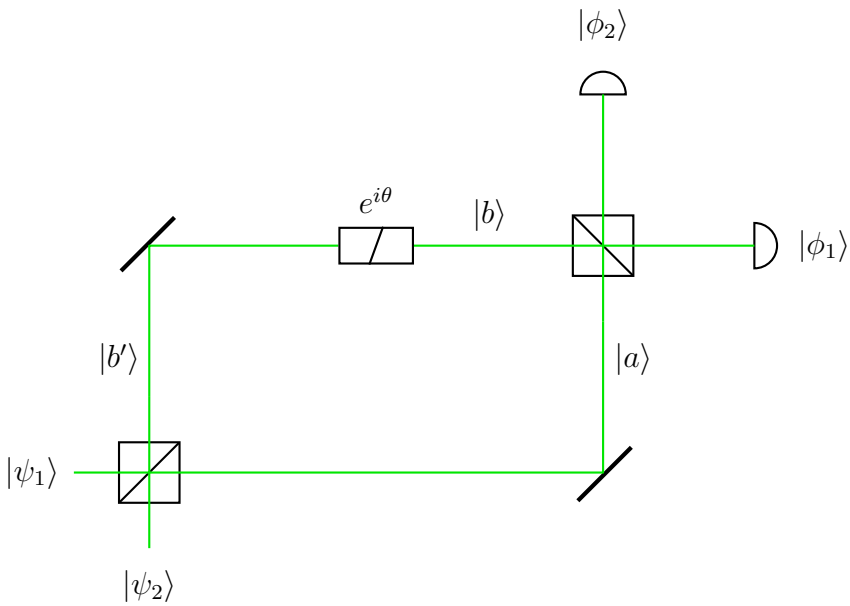


Figure 2.3: *Free-space Mach-Zehnder Interferometer.*

The interference in Figure 2.3 at point a, b and outputs ϕ_1 and ϕ_2, respectively, can be described using Dirac notation for some input ψ through

$$
\begin{aligned}
|a\rangle &= \frac{1}{\sqrt{2}}\left(|\phi_2\rangle + i|\phi_1\rangle\right) \\
|b\rangle &= \frac{1}{\sqrt{2}}\left(|\phi_1\rangle + i|\phi_2\rangle\right)
\end{aligned}
\tag{2.20}
$$

and for an phase modulator that adds a phase of θ

$$
|b'\rangle = e^{i\theta}|b\rangle \tag{2.21}
$$

the resulting wave function is given by

$$
\begin{aligned}
|\psi\rangle &= \frac{1}{\sqrt{2}}\left(|a\rangle + i|b'\rangle\right) \\
&= \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}\left[|\phi_2\rangle + i|\phi_1\rangle\right] + e^{i\theta}\left[\frac{1}{\sqrt{2}}\left(|\phi_1\rangle + i|\phi_2\rangle\right)\right]\right) \\
&= \frac{1}{2}\left[|\phi_2\rangle + i|\phi_1\rangle + ie^{i\theta}\left(|\phi_1\rangle + i|\phi_2\rangle\right)\right] \\
&= \frac{1}{2}\left[|\phi_2\rangle + i|\phi_1\rangle + ie^{i\theta}|\phi_1\rangle - e^{i\theta}|\phi_2\rangle\right] \\
&= \frac{1}{2}\left[\left(1 + e^{i\theta}\right)|\phi_1\rangle + i\left(1 - e^{i\theta}\right)|\phi_2\rangle\right]
\end{aligned}
\tag{2.22}
$$

thus, the probability of detecting a photon at output $|\phi_1\rangle$ respectively $|\phi_2\rangle$ at the outputs of the MZI given that it entered the at input $|\psi_1\rangle$ is given by

$$
\begin{aligned}
\left|\langle\phi_1|\psi\rangle\right|^2 &= \left|\left(\frac{1}{2}\right)\left(1 + e^{i\theta}\right)\right|^2 \\
&= \frac{1}{4}\left(1 + e^{-i\theta}\right)\left(1 + e^{i\theta}\right) \\
\left|\langle\phi_2|\psi\rangle\right|^2 &= \left|\left(\frac{1}{2}\right)\left(1 - e^{i\theta}\right)\right|^2 \\
&= \frac{1}{4}\left(1 - e^{-i\theta}\right)\left(1 - e^{i\theta}\right)
\end{aligned}
\tag{2.23}
$$

using the known identity

$$
e^{\pm i\theta} = \cos\theta \pm i\sin\theta \tag{2.24}
$$

the probabilities in Equation 2.23 can be rewritten as

$$\begin{aligned} \left|\langle\phi_1|\psi\rangle\right|^2 &= \frac{1}{2}\left(1+\cos\theta\right) \\ &= \cos^2\left(\frac{\theta}{2}\right) \\ \left|\langle\phi_2|\psi\rangle\right|^2 &= \frac{1}{2}\left(1-\cos\theta\right) \\ &= \sin^2\left(\frac{\theta}{2}\right) \end{aligned} \tag{2.25}$$

where ϕ_1 and ϕ_2 denote the state of a photon appearing at the upper and lower detector after entering the interferometer at ψ_1, respectively.

2.4.3 Interferometric Visibility and Distinguishability

The interferometric visibility is a measurement of the contrast of interference fringes in an interferometer as can be seen in Figure 2.4. It is a measurement quantifying the error in phase between the two arms of an interferometer when measured at either output of the beamsplitter where the both arms interfere. The visibility is defined as

$$v = \frac{I_{\max} + I_{\min}}{I_{\max} - I_{\min}} \tag{2.26}$$

so that

$$0 \leq v \leq 1$$

where $I_{\max}$ and $I_{\min}$ denote the maximum, respectively minimum intensity as measured at either of the outputs of the recombining beam splitter.

All interferometers are subject to time-varying intensity fluctuations stemming from fluctuations in the path length. Generally the intensity I at one of the detectors in the Mach-Zehnder interferometer in Figure 2.3 can be written as

$$I \propto 1 + \cos(\varphi(t)) \tag{2.27}$$

where $\varphi(t)$ is the change in phase angle over time. In fiber-optic interferometers the quantity $|\varphi(t)|$ depends largely on the environment [5], but fluctuations are present in bulk interferometers too.

Intensity and Probability of Quantum Measurements

The norm squared $\left|\langle\psi|\phi\rangle\right|^2$ of a quantum measurement that denotes the probability for one photon to be measured at a given detector as derived in Equation 2.25

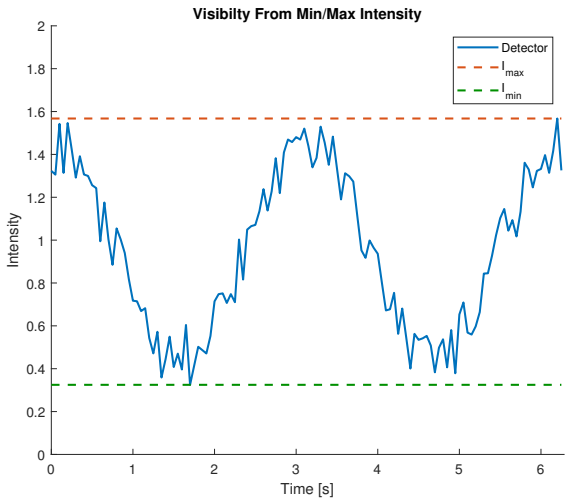


Figure 2.4: *Typical acquisition of minimum/maximum optical intensity to calculate visibility.*

is analogous to Equation 2.27 by

$$\begin{aligned} \cos^2\left(\frac{\theta}{2}\right) &= \frac{1}{2}\left[1+\cos\left(2\theta\right)\right] \\ &\propto \Big[1+\cos(\varphi(t))\Big]. \end{aligned} \tag{2.28}$$

As such, the probability of a measurement can be considered as the instantaneous probability for a single emitted photon to be detected at one of the detectors, while the intensity can be considered as the average over all measurements.

This means that the intensity is directly linked to having a stable reference frame for the quantum states. By substituting $\theta = \varphi\left(t\right)$ in Equation 2.25 it is apparent that the phase shift must be maintained constant for single photons to be reliably measured. Any random phase shift in the system gets added to the phase of all states, thus rotating the reference frame. Without cancelling that very phase shift, Bob will not be able to reliably decode the qubits.

By unifying Equation 2.25 and Equation 2.27 it has now been shown that having a stable intensity in a MZI when operating with a continuous-wave laser is equivalent to having predictable qubits when operating with single photons in the same MZI. Predictable photons means that the probability of detection at either arm is constant with respect to time.

Implication of High Visibility

The visibility dictates the depth of modulation that can be achieved. This implies that a high visibility is required to achieve good retention of the reference frame, such that qubits can be unambiguously measured, and further, that a drifting reference frame leads to a high QBER.

In QKD protocols such as BB84, the ability to detect an eavesdropper on the channel depends on measuring of the QBER as discussed in Section 2.2.2. If the visibility is low, so that the quantum channel is error-prone, then the additional error induced by an eavesdropper might get buried in the noise of the channel. This means that the presence of an eavesdropper cannot be detected with high probability.

2.5 Few-Mode Mach-Zehnder Interferometer

The controller will also be evaluated in a few-mode MZI (FM-MZI) where Alice's and Bob's interferometer halves in Figure 2.1 have been split up. Both the upper and the lower arms, which in the fiber-optic case consist of two fibers (single-mode), are multiplexed onto one so-called few-mode fiber (FMF). This allows for multiplexing of two optical channels onto one fiber cable through space-division multiplexing.

Figure 2.5 shows a FM-MZI where the upper and lower arms of Alice's half of the MZI enter a photonic lantern (PL) that multiplexes the arms onto one few-mode fiber. In this setup, a 750 meter FMF was used. The FMF is terminated in another PL that demultiplexes the signal into the two arms that make up Bob's half of the interferometer. Alice's upper arm has, similarly to Figure 2.1, an inline phase modulator and a polarization controller to adjust the polarization to the polarization-dependent phase modulator. Bob's half of the interferometer has polarization controllers in both arms to ensure retention of polarization reference frame.

Figure 2.6 shows the different spatial modes that were used. The plots can be seen as the cross-section of the fiber, where the heat map shows the probability for a photon to be found at that point of the cross-section. FM-fibers are a state-of-the art technique for multiplexing and can be combined with traditional forms of multiplexing like wavelength-division multiplexing or time-division multiplexing to further increase throughput through one fiber.

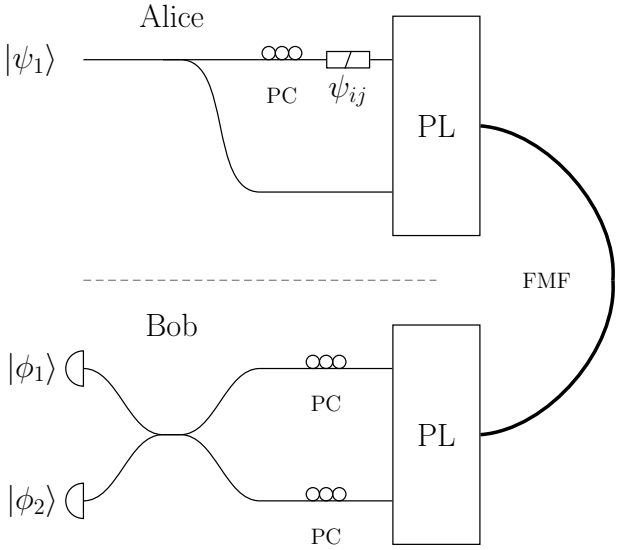


Figure 2.5: *Few-Mode Mach-Zehnder Interferometer as used in the experiment. The FPGA controls the phase modulator on Alice's half and the output from a detector on Bob's side closes the feedback path.*

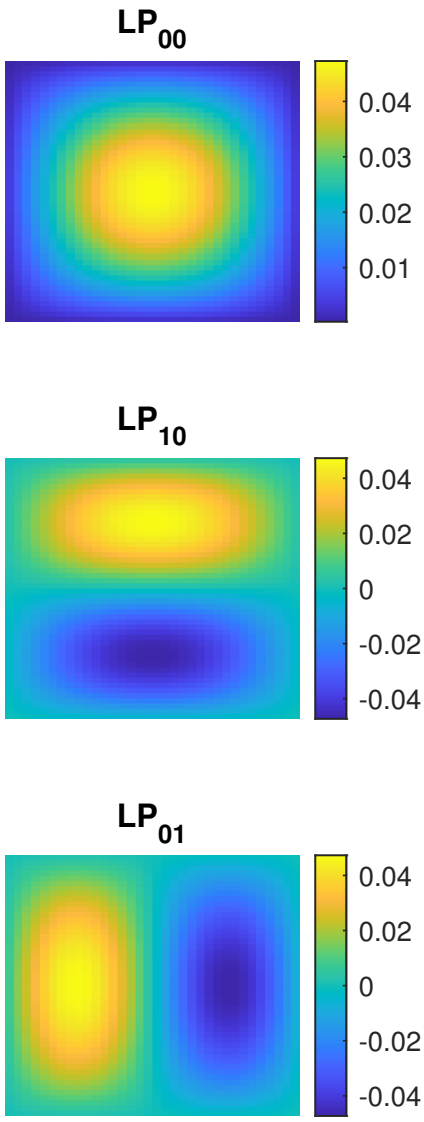


Figure 2.6: *Modes for Space-Division Multiplexing (Mode Multiplexing).*

3 Method

3.1 Experiment Setup

The experiment was carried out in a Mach-Zehnder interferometer assembled on a pneumatic optical table. The laser source was a 1546.917 nm telecommunication laser with an output power of +5.75 dBm and the fiber-optical connectors had a maximum insertion loss of 0.3 dB.

3.1.1 Fiber-Optical Mach-Zehnder Interferometer

The experimental system for phase compensation consists of a fiber-optic Mach-Zehnder interferometer where a laser source is connected to the upper arm of the first fiber-optic coupler. Both the upper and lower arm are connected to manual polarization controllers (PC), and the upper arm is subsequently connected to an electro-optic, polarization-maintaining, Lithium-Niobate modulator. Both arms of the interferometer are fed into a second beamsplitter where the interference occurs, after which the intensity is measured by an InGaAs-photoreceiver (detector) at the upper output of the beamsplitter. The electrical output is lowpass-filtered with a cutoff frequency $f_c = 1$ kHz to remove noise before the signal is fed into the control circuitry.

3.1.2 Alignment of Mach-Zehnder Interferometer

Careful alignment of the components of the interferometer has to be done in order to achieve high visibility (typically > 90% was achieved) of the interference fringes. With constant power and no applied voltage to the phase modulator the polarization controller in the upper arm was first adjusted to maximize the power after the phase modulator. The depth of modulation is dependent on the input

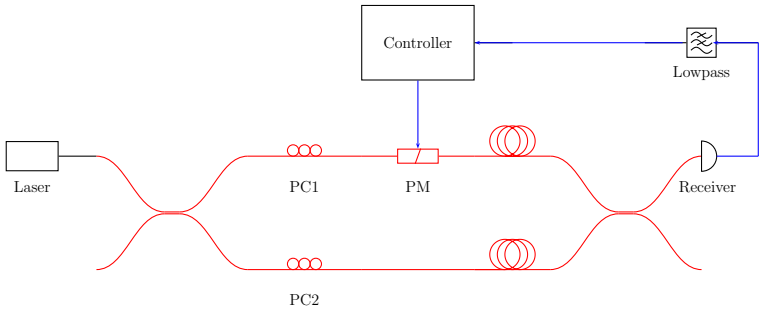


Figure 3.1: *Interferometer setup with optical (red) and electrical (blue) signals.*

polarization of the phase modulator. For some experiments an adjustable attenuator was adjusted to equalize the power between the output of the attenuator and the output of the phase modulator. This resulted in equal input power the the recombining beamsplitter. A sine wave was then applied to the phase modulator. The polarization controller in the lower arm was subsequently adjusted while observing the output of the photodetector. The polarization controller in the lower arm was adjusted to maximize the visibility of the interference fringes.

3.1.3 Optical Enclosure

The control algorithms 1 and 2 were evaluated both with and without an optical enclosure surrounding the interferometer. In the SA-MZI-setup the optical enclosure was a box of corrugated fiberboard, and in the FM-MZI-setup the optical enclosure was a box of acrylic glass.

3.1.4 Background Drift Characterization

The behavior of the interferometer system when uncontrolled was determined by disconnecting the phase compensation system and monitoring the output of the detector in the upper arm of the interferometer. The resulting fluctuations in optical intensity is deemed to be the background drift stemming from the environment.

3.1.5 Control Circuitry

The control circuitry in Figure 3.1 is based on an FPGA. The signal is output from the detector, $V_{\text{in}}(t)$, and is fed into a 12-bit ADC (analog-to-digital converter). The quantized value is read by the FPGA where the control algorithm is run and a control signal is outputted. The output control signal is fed to a 12-bit DAC (digital-to-analog converter) outputting a control voltage in the range $[0, 3.3]$ volts.

The phase modulator used has a half-period voltage $V_\pi = 7.5$ V and supports input voltages between $[-10, 10]$ volts. It is desirable for the phase controller to both be able to add, as well as subtract a phase shift to the arm, and thus a DC bias has to be added to the outputted voltage from the DAC. An operational amplifier is used, configured as a non-inverting summing amplifier with a gain of 1 to subtract a bias voltage of half the range of the DAC, thus obtaining the range $[-1.65, 1.65]$ volts.

This range however, is not sufficiently large excursion to reach the V_π voltage. Therefore, a non-inverting amplifier G with a gain of $G = 5$ is used to obtain the full excursion range $[-8.25, 8.25]$ volts. Finally, a custom driver stage was used to buffer the output signal in order to supply the current required by the phase modulator operating at 50Ω input impedance.

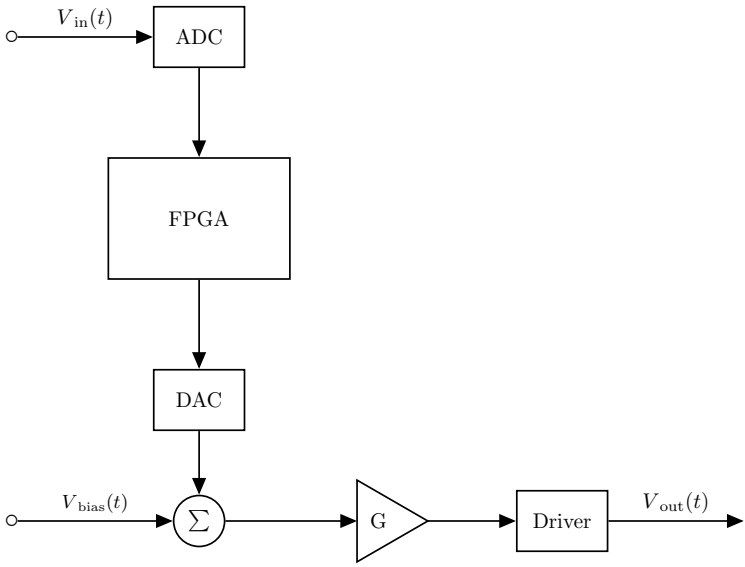


Figure 3.2: *Control circuitry with peripheral driving circuitry.*

3.2 Performance Metrics

In order to determine the effectivity of the control and to quantify the phase stability, a number of metrics have been borrowed from the area of statistics. The following metrics will be used.

3.2.1 Mean-Squared Error

The MSE between the samples $x[i]$ from the photodetector and the control loop setpoint is calculated

$$\text{MSE} = \frac{1}{N}\sum_{i=1}^{N}(x[i] - S)^2 \tag{3.1}$$

for some setpoint S, $\{S \in \mathbb{R} : 0 \leq S \leq 4095\}$. The constant 4095 corresponds to the $2^{12} - 1$ achievable quantization levels for the ADC that was used. The MSE quantifies how well the controller manages to hold the system at the setpoint. It is desirable to consider a metric of the system's fit to the setpoint that does not suffer from cancellation of the error due to summation of errors of different sign. It follows that squaring the error in each sample yields an error function where negative errors do not cancel out positive errors.

3.2.2 Standard Deviation

The SD σ measures the spread of the samples around an arithmetic mean μ, and is defined

$$\sigma = \sqrt{\frac{1}{N-1}\sum_{i=1}^{N}|x[i] - \mu|^2} \tag{3.2}$$

where $x[i]$ is the i:th sample. The standard deviation quantifies the spread of the samples in the signal from the photodetector. This can be seen as how jittery the signal is around some mean.

3.2.3 Performance Metric Discussion

While seemingly similar, both the MSE and SD are necessary to fully quantify how well-behaved the system is when subjected to external environmental noise. A high MSE and a low SD is indicative of a stable system, albeit with a stationary error. That is, the signal from the detector has a high correlation with the setpoint value, but is offset.

A low MSE and high SD is indicative of close adherence to the the setpoint, but that the output is subject to, what can be thought of as, high-frequency noise. I.e. the average of the signal is very close to the setpoint, but any instantaneous value for the sample has a high probability to be further from the setpoint.

3.3 Control Algorithms

This thesis investigates the application of two control algorithms, an incremental control algorithm ICA, and a proportional-, integral-, and derivative control

algorithm, PID.

3.3.1 Feedback Control

The control algorithms that were developed both were feedback-algorithms. The idea behind these algorithms is that the output of the controller is directly affected by previous values of the output and the controlled system's dynamic. A general model for a feedback control system is shown in Figure 3.3. G is the system to be controlled which in this thesis is the MZI. F is the controller including FPGA and driving circuitry.

A control error is formed as the difference between a desired value of the output $r(t)$ and the current output of the system $y(t)$. In this thesis, $y(t)$ corresponds to the output of the optical detector, and $r(t)$ to the setpoint.

If the transfer function for the system G is known, then the tunable parameters of the controller can be chosen to completely eliminate the control error [15]. In this thesis however, the transfer function of the system was unknown and tuning of the control gains was done experimentally.

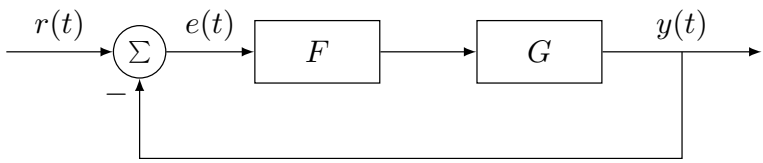


Figure 3.3: *Feedback control system.*

Both the ICA and the PID algorithm are examples of feedback control systems where the controller tries to drive the output of the closed loop system towards a setpoint value.

Selection of Setpoint

The setpoint for both ICA and PID was chosen to lie in the linear region of the interference pattern. This helped the controller maintain stability and reduce noise as as the derivative is approximately linear. At either the crest or the trough of the interference pattern a small step in either direction causes a change of the sign of the derivative. This means that for, example the ICA algorithm would be unstable around this point. Figure 3.4 shows a linearization and the target setpoint.

Consider for example a setpoint corresponding to a phase shift of π rad such that the derivative is 0. Then, the error term is very small for a small phase shift in either direction. That is, a small phase drift is yields a small control. The controller also runs the risk of saturating if it attempts to drive the applied phase shift to the equivalent setpoint at $\pi + 2\pi n$, $n \in \mathbb{Z}$.

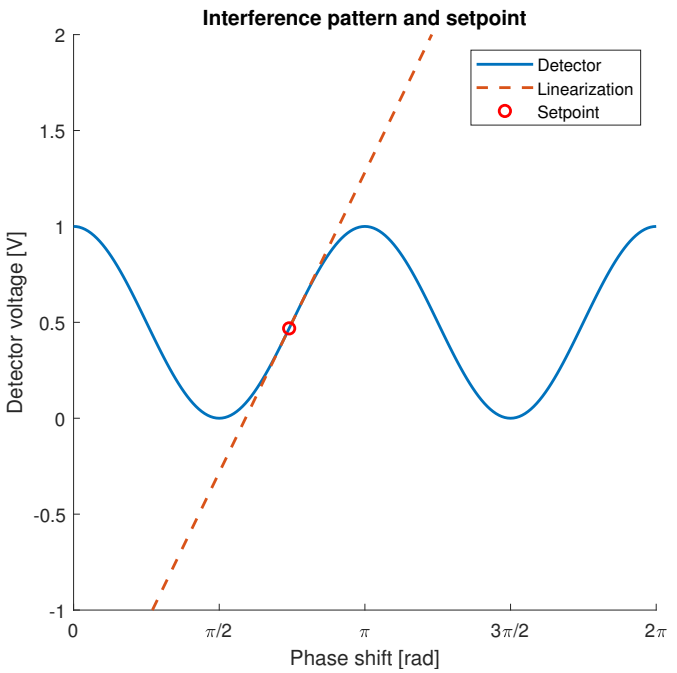


Figure 3.4: *Target setpoint in the interference pattern.*

Thus the setpoint was set to approximately halfway between the minimum and maximum amplitude of the optical signal.

3.3.2 Incremental Control Algorithm

The incremental algorithm described in Algorithm 1 considers the change in error between a setpoint value and current input value to the controller. While the error is decreasing, the controller increments or decrements the output value by a chosen step size. If the new error is greater than the error in the previous iteration, the direction of the counter is reversed such that the output value is driven in the opposite direction. This type of controller is a very basic controller and among one of the simplest control algorithms.

This algorithm is thought to perform well under conditions of high uncertainty about the system as it needs no other information than the current and the previous error. However, the step size is static implying that the controller will oscillate around the setpoint value. To overcome this, hysteresis is added and treated as a tunable parameter.

Hysteresis

To eliminate jitter around the setpoint with the ICA-controller, hysteresis was added. This was implemented as a lower bound on the error before the controller

began actuating. That is, if the error (Figure 3.3) $|e(t)| > \delta$ for some tunable hysteresis parameter δ, the controller began incrementing or decrementing the counter and consequently also driving the output voltage. If the error $|e(t)| < \delta$ the controller was idle.

Tuning of ICA Parameters

The step size and hysteresis were tuned experimentally while observing the interference pattern over time on a DSO. The step size was increased until the system started oscillating and then subsequently reduced to reduce oscillations. Any residual oscillations were eliminated by increasing the hysteresis.

However, care was taken to keep the hysteresis minimal to minimize the interval in which the system was allowed to fluctuate before actuating the controller.

3.3.3 PID-Controller

The use of an FPGA with a constant clock speed simplifies the implementation of the PID-algorithm. Calculation of integral and derivative terms is simplified from the conventional continuous-time PID-algorithm which is defined as

$$y(t) = K_P \cdot e(t) + K_I \cdot \int_0^t e(\tau)\,\mathrm{d}\tau + K_D \cdot \frac{\mathrm{d}e(t)}{\mathrm{d}t} \tag{3.3}$$

where $e(t)$ is the error defined as $e(t) = r(t) - y(t)$ for some setpoint $r(t)$ and system output $y(t)$ into

$$y[n] = K_P \cdot e[n] + \overline{K}_I \cdot \sum_{k=0}^{n-1} e[k] + \overline{K}_D \cdot (e[n] - e[n-1]) \tag{3.4}$$

where $e[n]$ is the error term at time step n defined as $e[n] = r[n] - y[n]$. Since Δt is constant it can be factored into $\overline{K}_I$ and $\overline{K}_D$, thus removing the differentials. Algorithm 2 describes the implementation of the discrete-time PID-algorithm used.

Tuning of PID Parameters

The parameters K_P, K_I and K_D were tuned experimentally while observing the interference pattern over time on a DSO. The proportional gain was gradually increased until pronounced oscillations were seen in the interference pattern. The proportional gain was lowered until the oscillations ceased. If a steady-state error was noticed, the integral term was increased until the either the steady-state error was eliminated or the system started oscillating again. If oscillations started, the integral gain was again lowered. If any residual oscillations remained the derivative gain was increased.

Algorithm 1 Incremental Control Algorithm

```
output ← 0
direction ← INCR
error ← 0
old_error ← 0
input ← 0
while True do
    input ← read_adc()
    error ← abs(setpoint – input)
    if error < hysteresis then                ▷ Only act if error is sufficiently large
        if error ≥ old_error then
            if direction = INCR then                                  ▷ Reverse direction
                direction ← DECR
            else if direction = DECR then
                direction ← INCR
            end if
        end if
        if direction = INCR then
            output ← output + step_size
        else
            output ← output - step_size
        end if
        if output > 4095 then                 ▷ Return to midpoint on saturation
            output ← 2048
        else if output < 0 then
            output ← 2048
        end if
        write_dac(output)
    end if
end while
```

Algorithm 2 PID Control Algorithm

```
output ← 0
error ← 0
old_error ← 0
input ← 0
P ← 0
I ← 0
D ← 0
while True do
    input ← read_adc()
    error ← setpoint − input
    P ← K_P · error
    I ← K_I · (old_error + error)
    D ← K_D · (old_error − error)
    output ← K_P + K_I + K_D
    if output > 4095 then                ▹ Saturate to prevent overflow
        output ← 4095
    else if output < 0 then
        output ← 0
    end if
    write_dac(output)
end while
```

3.4 FPGA-circuit

The controllers described in Section 3.3 were implemented on a Xilinx Zynq-7000 system-on-chip (SoC). The Zynq-board is a SoC that contains both conventional FPGA-fabric and an ARM-processor.

The control algorithms were implemented in the FPGA-fabric, but parametrized such that the algorithm parameters were settable from a program. The processor runs a bare-metal program which handles UART-communication with a host PC for setting the parameters and for monitoring. The FPGA-fabric is organized into different blocks based on function. Each block is then implemented using VHDL. Figure 3.5 show the component layout and the inter-block communication. A full block diagram over the components can be found in appendix A.1.

The development board that was used has an on-board clock source operating at 100 MHz. This was divided to two clock signals at 50 MHz, and 25 MHz respectively.

3.4.1 ADC-/DAC-block

Communication with the ADC and DAC was done through an SPI-like interface. The 25 MHz clock signal is used by the ADC/DAC which is limited by hardware. A serializer and deserializer had to be implemented in order to exchange data with the converters. The serializer serializes a 12-bit word after adding a preamble by shifting it out to the converter. Likewise, the deserializer shifts in a preamble and data to convert it into a 12-bit word.

Both the ADC and DAC are operating untriggered such that they are constantly outputting at maximum clock speed. This removes the need for synchronizing writing and reading from the controller, as the operating speed of the ADC and DAC is much faster than period time of the control loop.

3.4.2 Controller block

The controller block contains the implementation of algorithms 1 and 2. The 50 MHz clock signal is further divided down in the controller block. The clock is divided by a factor of 2^n where n is a parameter that is settable from the control software. This allows for the operating speed of the controller to be adjusted. This is directly linked to the gains of the control algorithms. A control algorithm that is operating at a lower frequency will read a larger error term as the system G has drifted. This will lead to oscillations if the gains are too large. Care has to be taken to tune the clock prescaler so that the controller is sufficiently fast to react to disturbances, but also so that a too high clock speed does not result in noisy signals.

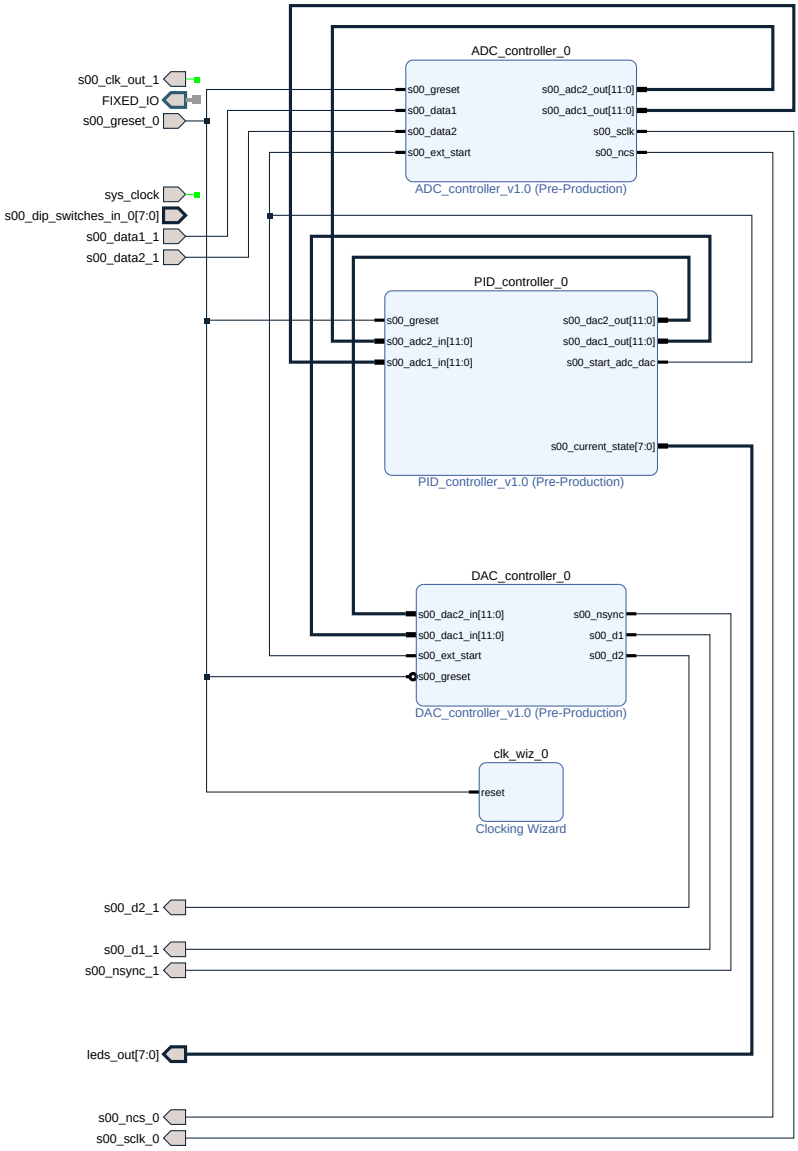


Figure 3.5: *Component view of FPGA-fabric. Data buses are shown by bolded lines and scalar signals in in normal width.* ADC_controller_0 *is the serializer that converts a* 12*-bit data word to a preamble and serial data.* DAC_controller_0 *is the deserializer that converts a preamble and serial data into a* 12*-bit data word.* PID_controller_0 *is the main controller block. Here the* PID *version is shown.* clk_wiz_0 *is the clock divider discussed in Section 3.4.*

4

Results and Discussion

This chapter presents the experiment results for an SA-MZI and FM-MZI as described in Chapter 3 controlled by the algorithms incremental control algorithm (ICA, Algorithm 1) and proportional-, integral-, derivative- (PID, Algorithm 2).

4.1 Stand-Alone MZI

Figure 4.1 shows the output of the detector in the upper arm where the controller is turned off after $t = 25$ seconds. When the controller is turned off the interferometer is left free-floating and it immediately starts drifting. The oscillations that start after $t = 25$ seconds are due to the sinusoidal background drift. This strongly shows the need for active control, and in conjunction with Figure 4.2a and Figure 4.2b it shows that passive control is not sufficient as the interferometer promptly drifts when uncontrolled.

4.1.1 Phase Drift Without Control

Figure 4.2 shows the output of the detector in the upper arm. It shows how the interference varies over time with, and without, enclosure.

By plotting the time series in a histogram, the distribution of samples can be shown. Figure 4.3 shows the distribution of the background noise in Figure 4.2. The background drift in Figure 4.2 clearly shows that an unstabilized MZI is not well-suited for use in QKD experiments. The noise in Figure 4.2b shows dampened oscillations when compared to Figure 4.2a. However, there is still residual drift that needs to be compensated for.

Further, the histograms in Figure 4.3a and Figure 4.3b show that the distribu-

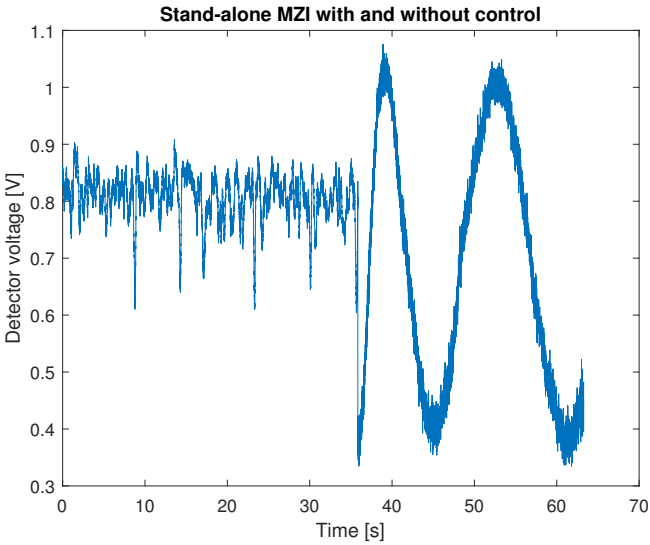
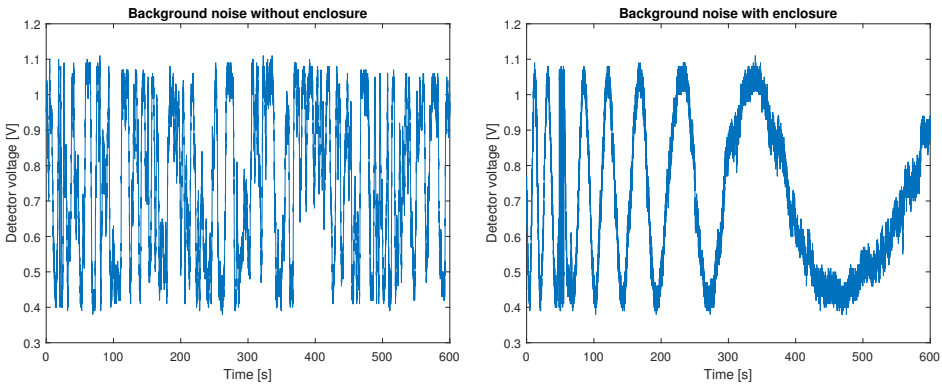


Figure 4.1: *Detector and phase modulator plot of an PID-controlled SA-MZI with enclosure and control turned off at $t = 35$ seconds.*

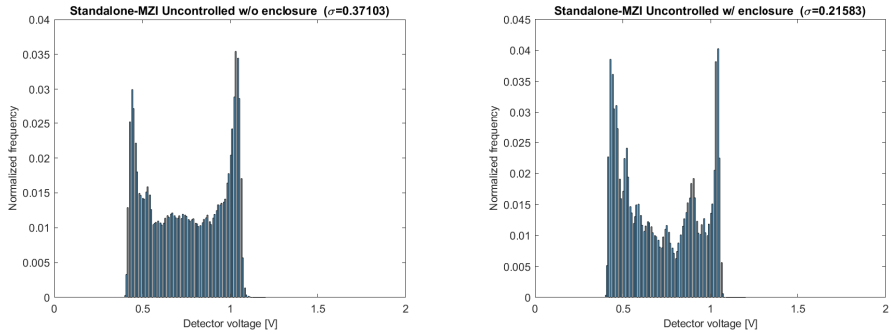


(a) *Without enclosure.* ***(b)*** *With enclosure.*

Figure 4.2: *Background drift for an SA-MZI.*

tion of samples is not uniform. That is, the background drift is not white. Two large peaks exist at around 0.4 volts, and again a similar peak at around 1.2 volts in both the unenclosed an enclosed setups. This further shows the sinusoidal pattern of the background drift, and that the samples are concentrated at the minimum and maximum values of the sine wave that corresponds to the phase drift. There is a central spike in Figure 4.3b, and the reason for this is not known.

Figure 4.3a and Figure 4.3b also clearly show that only using an enclosure is not



(a) *Without enclosure.* ***(b)*** *With enclosure.*

Figure 4.3: *Histogram over the distribution of samples for an SA-MZI.*

sufficient to obtain a low spread spread of samples from the detector. By combining the enclosure with a control algorithm, the total stability is improved, as can be seen in Section 4.3. The figures show that, while there is a slight difference between having a the interferometer enclosed versus not having it enclosed, there is not much improvement.

4.1.2 Stand-Alone MZI with PID-controller

The following section presents results from an experiment with the PID-controller in an SA-MZI configuration operating with, and without, enclosure.

Without enclosure

Figure 4.4 shows the time series of the output of the detector in the upper arm (upper plot), and the time series of the signal to the modulator (lower plot). There is still some residual drift as can be seen in the upper plot of the detector signal. This residual drift can be attributed to suboptimal tuning of the PID parameters, and it is believed that more derivative There are spikes in the detector signal, and those are believed to be caused by the system drifting outside of the phase modulators actuation range, but the controller manages to recover from this as the background drift is periodic.

A histogram of the time series of the signal from the detector in Figure 4.4 can be seen in Figure 4.5. Here, an improvement can be seen by comparing Figure 4.5 with the histogram of the interferometer (Figure 4.3) without phase control.

With enclosure

There is a clear improvement of the oscillations in Figure 4.6 when compared to Figure 4.4. The plot of the modulator voltage also shows that the controller actuates less than in Figure 4.4, which can be attributed to less high-frequent fluctu-

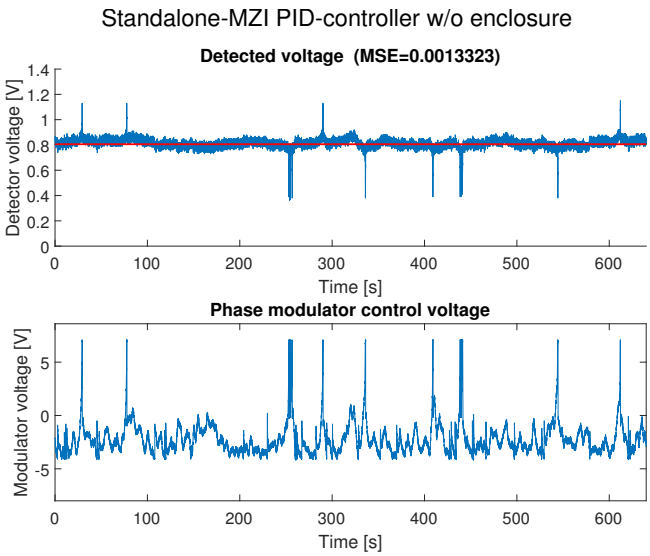


Figure 4.4: *Detector and phase modulator plot of an PID-controlled SA-MZI without enclosure.*

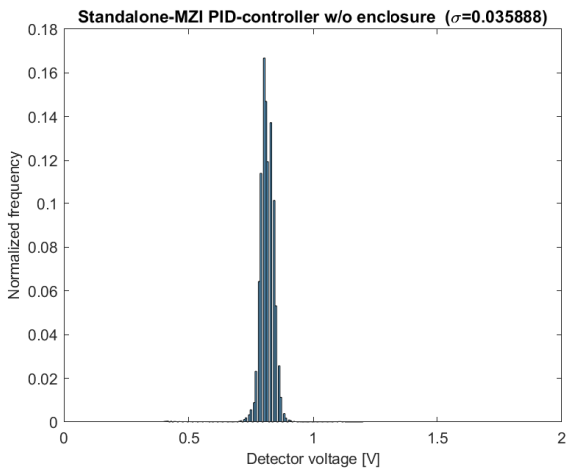


Figure 4.5: *Histogram over the distribution of samples for an PID-controlled SA-MZI without enclosure.*

ations when the system is enclosed. There is a spike at around $t = 330$ seconds in the plot of the detector signal. This is most likely caused by an electrostatic discharge in the laboratory. The detector is very sensitive, and when electrostatic discharges occur it shows up as noise on the detector. This spike is fed back to the the controller which causes the signal to the modulator to also increase. However,

the controller can recover from this spike as can be seen in the plots in Figure 4.6. Comparing the histogram in Figure 4.7, an improvement can be seen over the

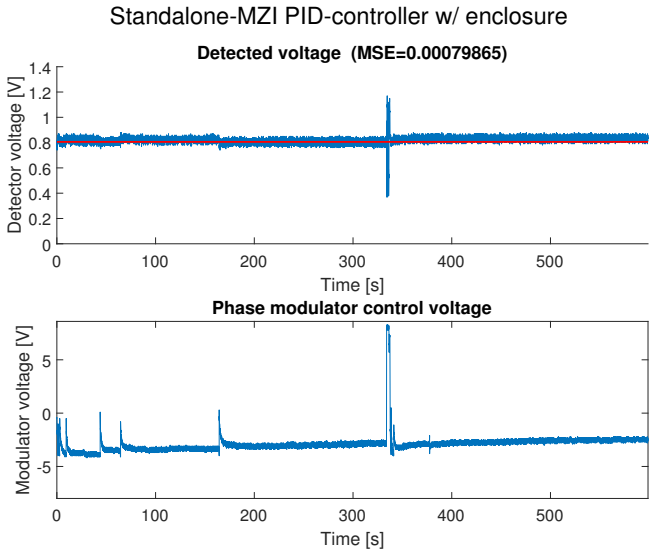


Figure 4.6: *Detector and phase modulator plot of an PID-controlled SA-MZI with enclosure.*

unenclosed case (Figure 4.5) in terms of spread of the samples.

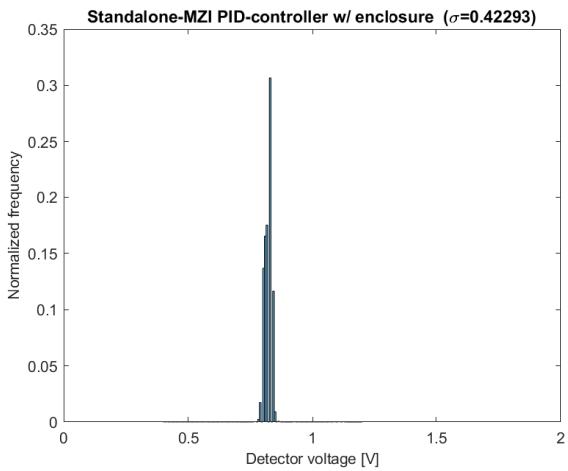


Figure 4.7: *Histogram over the distribution of samples for an PID-controlled SA-MZI with enclosure.*

The PID-controller also performs better when used in conjunction with an enclosure. Figure 4.4 and Figure 4.6 show that similarly to the ICA-controller, the

PID-controller saturates less when used in an enclosure. Saturation in this case refers to the output value reaching the maximum addressable of the DAC so that the output signal clips.

4.1.3 Stand-Alone MZI with ICA-controller

The following section presents results from an experiment with the ICA-controller in an SA-MZI configuration operating with, and without, enclosure.

Without enclosure

When operating without enclosure, the ICA-controller actuates the phase modulator a lot which can be seen in Figure 4.8. The discontinuities in the output signal to the modulator show the resetting behavior of the algorithm. That is when the controller is about to saturate either up or down, and subsequently resets the output counter to its starting value. Sometimes, this reset does not correspond to a phase shift of one half period of the background drift. This results in spikes being induced in the output of the detector, which can be seen in the plot of the detected voltage signal. These spikes are more frequent when the interferometer is unenclosed than when it is enclosed. However, the controller manages to recover from this. At around $t = 580$ seconds, artifacts can be seen in both the plot of the detected voltage as well as the output to the phase modulator. This is also thought to be due to electrostatic discharges as discussed in Section 4.1.2.

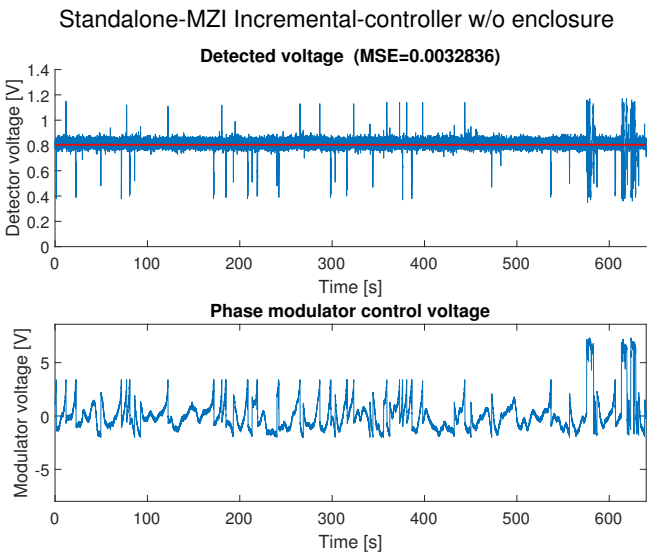


Figure 4.8: *Detector and phase modulator plot of an ICA-controlled SA-MZI without enclosure.*

The histogram in Figure 4.11 shows a clear improvement over the uncontrolled case (Figure 4.3). Comparing this to the PID-controller operating without en-

closure, this performs better in terms of sample spread. This can probably be attributed to the fact that the ICA-controller is more aggressive than the PID-controller, due to fixed step sizes when incrementing the output counter. This leads to the controller being more responsive, but also more likely to overshoot and oscillate in a region close to the setpoint.

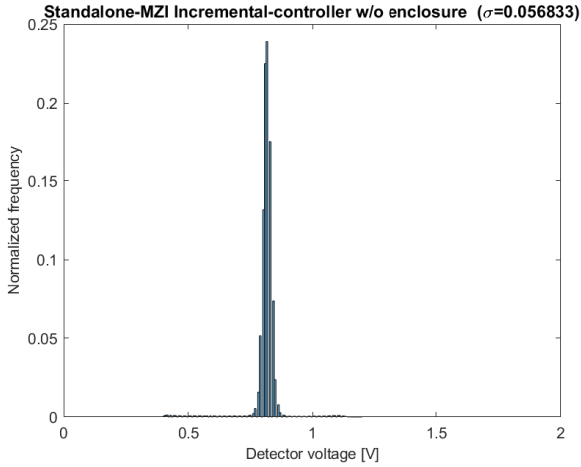


Figure 4.9: *Histogram over the distribution of samples for an ICA-controlled SA-MZI without enclosure.*

With enclosure

Operating with enclosure, the ICA-controllers performs less resets, and the output signal to the modulator is more stable as can be seen in Figure 4.10. The resets are fewer, and more spaced out compared to Figure 4.8. This is most likely due to the background drift being more slow-changing when the interferometer is enclosed. Similar behavior can be observed with the PID-controller in Figure 4.6. The ICA-controller also manages to hold the setpoint well and can recover from the few resets that occurs in Figure 4.10.

The histogram in Figure 4.11 also shows an improvement over the uncontrolled interferometer in Figure 4.3. The differences between the distribution of samples in the unenclosed ICA-controller and the enclosed ICA-controller are small and nonsignificant.

The spread of samples shown in the histograms in Figure 4.9 and Figure 4.11 show a slight worsening in SD when operating in an enclosure. The reason for this is yet unknown.

The ICA-controller has lower MSE and SD than the PID-controller when operating with enclosure. However, the difference in SD between SA-PID and SA-ICA indicates that SA-PID only is marginally better.

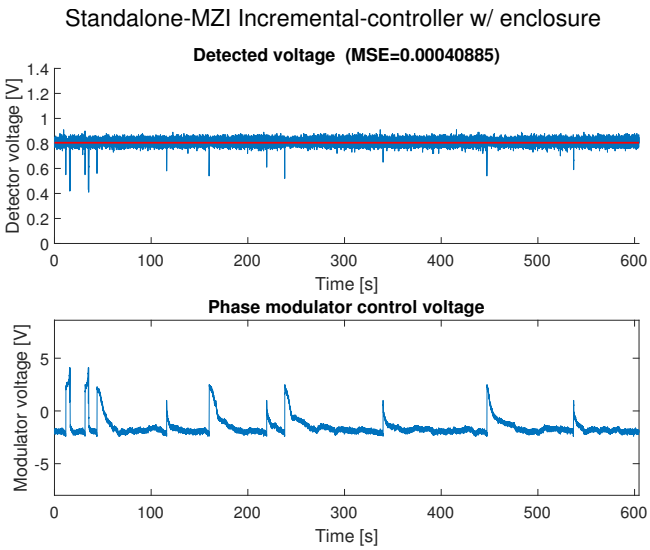


Figure 4.10: *Detector and phase modulator plot of an ICA-controlled SA-MZI with enclosure.*

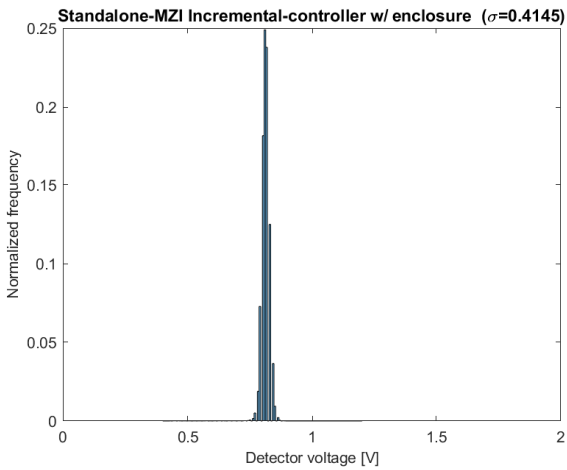


Figure 4.11: *Histogram over the distribution of samples for an ICA-controlled SA-MZI with enclosure.*

4.2 Few-Mode MZI

The following section presents results from an experiment with the PID-controller in an FM-MZI configuration operating with, and without, enclosure. This section also presents results from measurements of the background drift in the same interferometer.

4.2.1 Background Drift Uncontrolled

Figure 4.12 shows the background drift for a few-mode MZI. The drift has a strong sinusoidal appearance which is then dampened slightly before half the experiment duration. It is not known why the drift is irregular, but the FM-MZI is assembled with more components, compared to the SA-MZI, which are all sources of noise. This might be the cause for this drift, but more work needs to be done in order to fully characterize the sources of noise in this configuration.

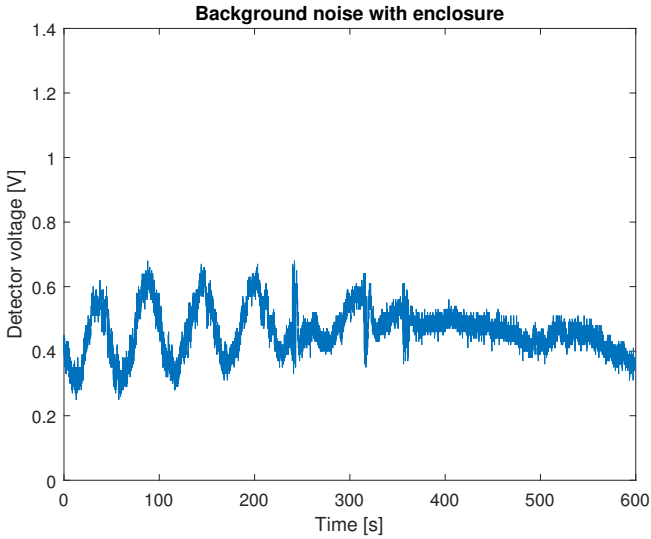


Figure 4.12: *Background drift in a FM-MZI.*

The background drift, as can be seen in Figure 4.13 does not resemble Figure 4.3, and the reason for this is yet unknown for the same reason as mentioned above. This irregularity suggests that the drift is neither sinusoidal nor white, but more work needs to be done in order to fully characterize this.

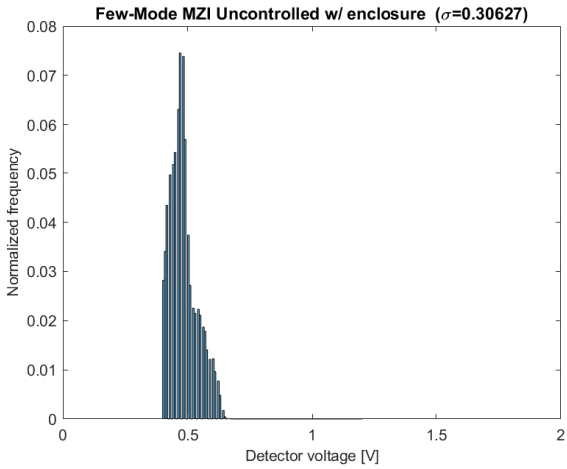


Figure 4.13: *Histogram over the distribution of samples for the background drift for an FM-MZI with enclosure.*

4.2.2 Few-Mode MZI with PID-controller

With enclosure

The PID-controller can phase lock the FM-MZI as can be seen in Figure 4.14. The plot of the output from the detector shows a small rollover at around t = 500 seconds. The reason for this is yet unknown. A significant steady-state error can be observed. The reason for this is unknown. This steady-state error significantly increases the MSE.

The same output power was used for both the SA-MZI and the FM-MZI, and the latter has higher power losses due to more components, so the contrast between the fluctuations are not as pronounced. That is, the amplitude of the fluctuations is significantly lower, and since the error term in the PID-controller is formed from the output term it might impact how much the output signal varies with each iteration of the control loop.

A clear improvement can be seen in Figure 4.15 over the uncontrolled case in Figure 4.13. The distribution is narrower around the setpoint as compared the same interferometer uncontrolled.

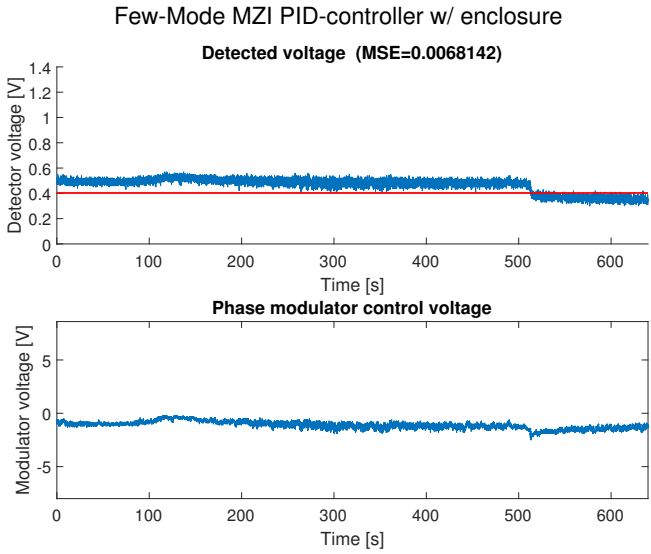


Figure 4.14: *Detector and phase modulator plot of an PID-controlled FM-MZI with enclosure.*

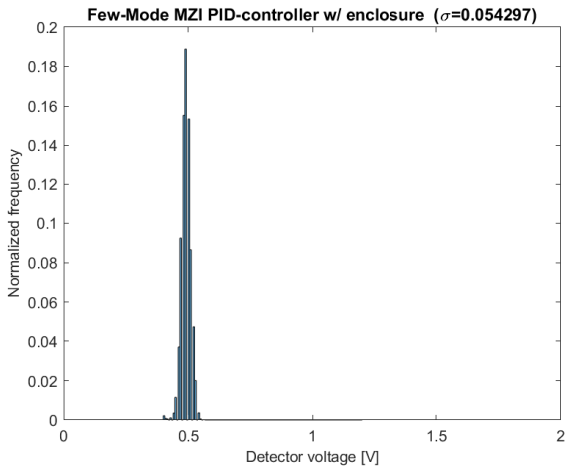


Figure 4.15: *Histogram over the distribution of samples for an PID-controlled FM-MZI with enclosure.*

4.3 Quantitative Comparison

This section summarizes the metrics as defined in Chapter 3 for the experiment setups in sections 3.1.4-4.2.

4.3.1 Mean Squared-Error

Controller	No enclosure	Enclosure
SA-PID	0.00133323	0.00079865
SA-ICA	0.00328360	0.00040885
FM-PID	-	0.00681420

Table 4.1: *Mean squared error as defined in equation between the setpoint and the optical output.*

4.3.2 Standard deviation

Controller	No enclosure	Enclosure
SA-uncontrolled	0.371030	0.21583
SA-PID	0.035888	0.422930
SA-ICA	0.056833	0.414500
FM-PID	0.306270	0.214490

Table 4.2: *Standard deviation as defined in Equation 3.2.*

4.3.3 Setpoint

Controller	No enclosure	Enclosure
SA-PID	800 mV	800 mV
SA-ICA	800 mV	800 mV
FM-PID	-	400 mV

Table 4.3: *Values for the setpoint used for ICA and PID.*

4.4 General Discussion

Contribution

To the best of the author's knowledge, this thesis is the first investigation of active phase control of a FM-MZI. It also features the first comparison of a ICA-algorithm with a PID-algorithm in a SM-MZI, and the first application of a PID-algorithm in a FM-MZI. The work in this thesis lays a foundation for further experiments where phase stability is a prerequisite. The control hardware also forms a platform on which further phase-coding experiments can be performed, as the FPGA-circuitry easily can be extended to also encode qubits in addition to controlling the phase.

Method and Applicability for Future Work

Successfully achieving phase stability on an optical table with long fiber-optic cables under less-than-ideal conditions is thought to generalize well. That is, a system that is capable of phase-locking a fiber-optic interferometer is thought to also be able to phase-lock a bulk interferometer. Due to experimental limitations, the FM-MZI could not be evaluated in an unenclosed configuration. It is not known to which extent this limits reproducibility. The control algorithms can be reproduced from the algorithm descriptions (Algorithm 1, Algorithm 2) without the need for the (highly vendor-specific) source code that was developed in this thesis.

5 Conclusions

The results in Chapter 4 clearly show that phase stability can be achieved over long time in a fiber-optic Mach-Zehnder interferometer with an FPGA by actuating a phase modulator. This is a prerequisite for future experiments with quantum key distribution.

It has also been shown that external control circuitry has to be used in conjunction to an FPGA with an ADC/DAC to amplify the signal to the phase modulator. The results also show that both a PID-algorithm and an ICA-algorithm can be used to stabilize an interferometer with significant improvement over an uncontrolled interferometer (Figure 4.1). It has also been shown that an improvement of phase stability can be achieved in a spatially multiplexed FM-MZI when compared to the same configuration uncontrolled. The results, however, are not conclusive as the number of error sources are considerably higher in a FM-MZI than in a stand-alone MZI.

It has also been shown that the effect of optical enclosures is that the MSE is reduced while the SD is increased when combined with a PID-controller or a ICA-controller. The impact of optical enclosure improves both the MSE by about an order of magnitude, while the SD increased by about an order of magnitude when used with an enclosure. More work has to be done to fully characterize this behavior.

5.1 Future Work

Future work include evaluating the system online in a system during data transmission over a quantum channel. This would be done by synchronizing the phase drift of Alice's and Bob's interferometers, and also ultimately performing sifting,

reconciliation and privacy amplification on the same FPGA device. This would allow for quantification of the quantum bit-error rate, QBER in order to fully evaluate the practical stability.

Multiplexed Communications Channel and Control Channel

This thesis only considers the usage of phase compensation with single-mode fibers without multiplexing, i.e. data modulation and phase compensation is done on the same optical channel. The drawback of this is that optical intensity is not a good measurement of phase stability in the feedback loop if phase coding is used, as the detection of optical intensity depends on the relative phase, which is indiscernible from phase fluctuations due to modulation. Further work in this area would include using a dedicated channel for sensing phase stability, either through WDM or through multi-mode fibers. The detection of phase stability would thus not be affected by the encoding of quantum states and accurate readings of the stability could be achieved.

Adaptive Control Algorithms

It would also be interesting to investigate the possibility of using adaptive algorithms (i.e. machine learning) to automatically tune the control parameters which have thus far been manually set according to some heuristic. This could be especially promising since the overview of the background drift in Figure 4.3 shows some regularity in the background drift, which could imply that a model can be fit to the characteristics.

Appendix

A

FPGA Block Diagrams

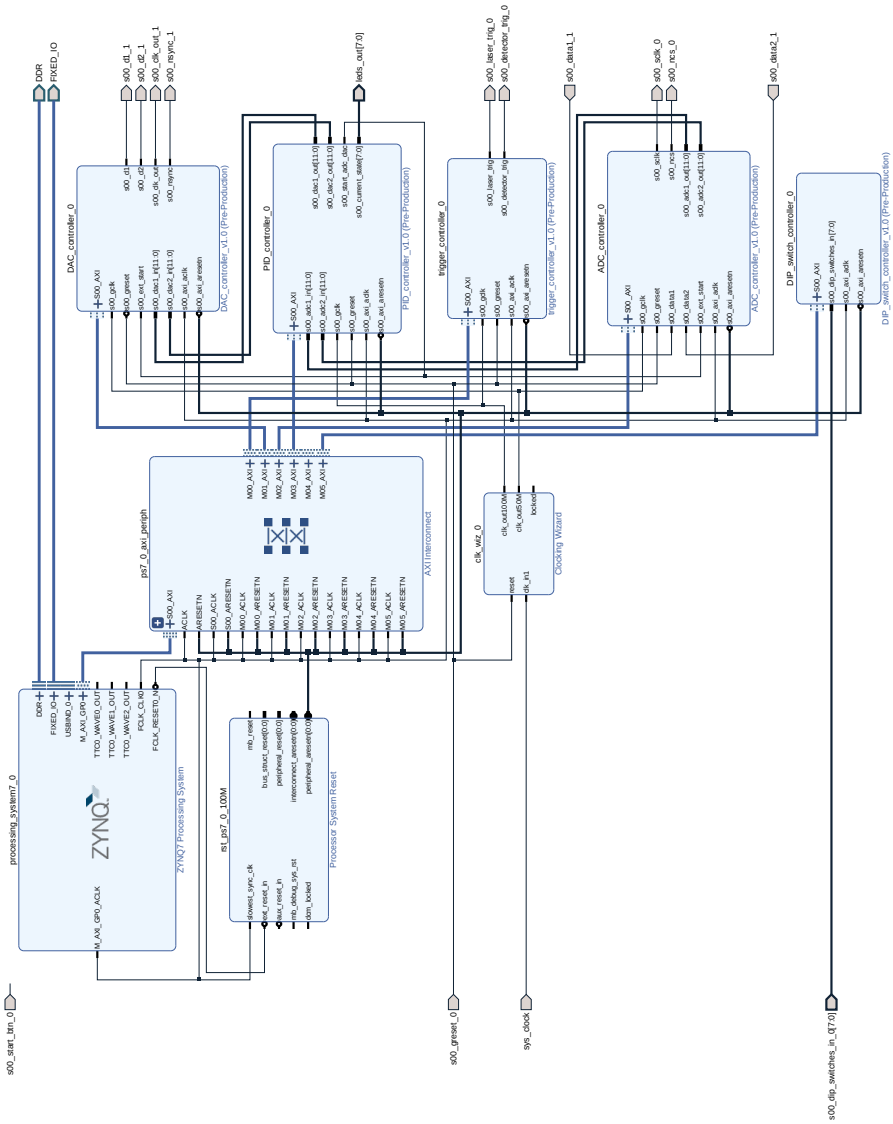


Figure A.1: *Full system overview with inter-block communication.*

B

Photograph: Control Electronics

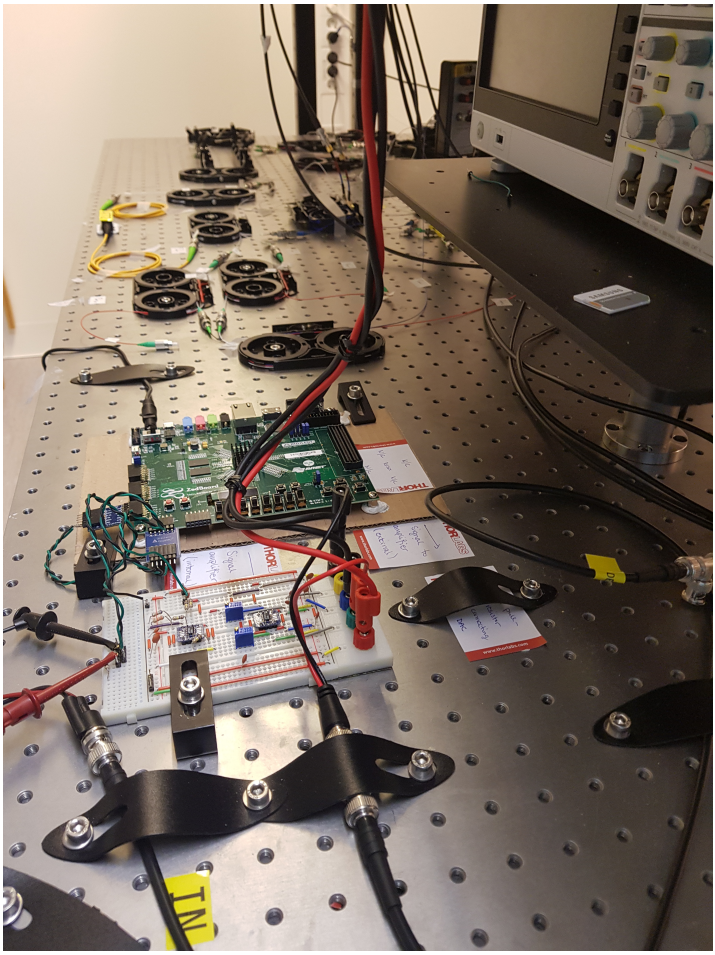


Figure B.1: *Interferometer setup with driving circuit on breadboard (white, lower left corner), FPGA-circuit (green, middle), and spool-wound beam-splitters and optical fibers (black, background). The signal from the detector (bottom left), and the output to the phase modulator (bottom right) are connected through BNC-cables. Data acquisition is done using a DSO (top right). Cables entering from the top (top center) supply power to the amplifiers.*

C

Photograph: Interferometer Setup

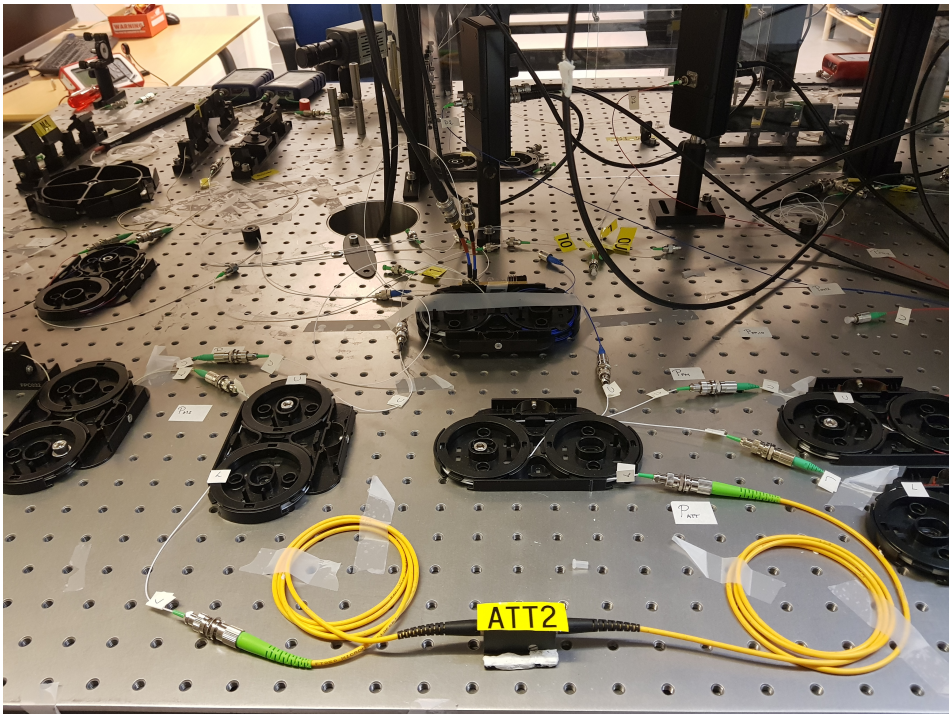


Figure C.1: *Light rom the polarization controllers of the upper and lower arm enter fibers into the phase modulator (center), and the attenuator (bottom center). Excess cable is wound up on a fiber spool (lower center), and is subsequently connected to a 90/10-beamsplitter (bottom/mid right) before the 90%-outputs are connected to photoreceivers (middle/right top).*

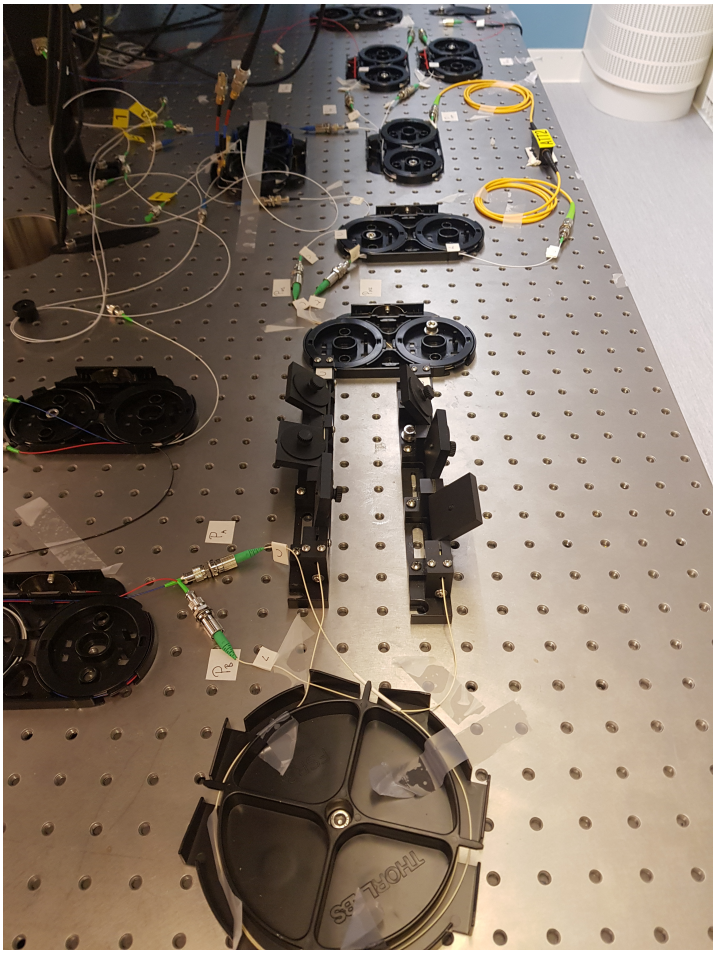


Figure C.2: *The two arms of a* SA-MZI*. Light enters from the first beamsplitter (bottom left), excess fiber of the upper and lower arm is wound up on a fiber spool (bottom center). Excess fiber after the polarization controller of the upper beam (leftmost) is wound up on a fiber spool, before being connected to the phase modulator (top left). The bottom arm's polarization controller (rightmost) is connected to an attenuator (yellow fiber) after the excess fiber is wound up on a fiber spool. The outputs of the attenuator and phase modulator is connected to two 90/10 beam splitters (top center) in both arms where the 10%-output is used for power measurement during operation. The 90%-outputs are connected to a recombining beamsplitter (topmost center) and the outputs of the beamsplitter are connected to two photoreceivers (not visible).*

Bibliography

[1] Simon Singh. *The Code Book: The Evolution of Secrecy from Mary, Queen of Scots, to Quantum Cryptography*. Doubleday, 1st edition, 1999. ISBN 0385495315.

[2] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J. Cerf, Miloslav Dušek, Norbert Lütkenhaus, and Momtchil Peev. The security of practical quantum key distribution. *Rev. Mod. Phys.*, 81:1301–1350, September 2009. doi: 10.1103/RevModPhys.81.1301.

[3] Feng Gao. Interferometry for online/in-process surface inspection. In *Optical Interferometry*. InTech, February 2017. doi: 10.5772/66530.

[4] XiaoMing Lu, LiJun Zhang, YongGang Wang, Wei Chen, Dajun Huang, Deng Li, Shuang Wang, DeYong He, ZhenQiang Yin, Yu Zhou, Cong Hui, and ZhengFu Han. Fpga based digital phase-coding quantum key distribution. *Science China*, 58(12), 2015. doi: 10.1007/s11433-015-5742-z.

[5] G.B Xavier and J. P. von der Weid. Stable single-photon interference in a 1 km fiber-optic mach–zehnder interferometer with continuous phase adjustment. *Optics Letters*, 36(10), 2011. doi: 10.1364/OL.36.001764.

[6] Cho Seok-Beom and Noh Tae-Gon. Stabilization of a long-armed fiber-optic singlephoton interferometer. *Optics Express*, 17(21), 2009. doi: 10.1364/OE.17.019027.

[7] Xiao-Song Ma, Stefan Zotter, Nuray Tetik, Angie Qarry, Thomas Jennewein, and Anton Zeilinger. A high-speed tunable beam splitter for feed-forward photonic quantum information processing. *Optics Express*, 19(23):22723, 2011. ISSN 1094-4087. doi: 10.1364/oe.19.022723.

[8] Frank Rubin. One-time pad cryptography. *Cryptologia*, 20(4):359–364, 1996. doi: 10.1080/0161-119691885040.

[9] Fu-Guo Deng and Gui Lu Long. Secure direct communication with a quantum one-time pad. *Phys. Rev. A*, 69:052319, May 2004. doi: 10.1103/PhysRevA.69.052319.

[10] Charles H Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. *International Conference on Computers, Systems & Signal Processing, Bangalore, India, Dec 9-12, 1984*, pages 175–179, December 9-12 1984. doi: 10.1016/j.tcs.2014.05.025.

[11] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299(5886):802–803, 1982. ISSN 00280836. doi: 10.1038/299802a0.

[12] S. Roman. *Advanced Linear Algebra*. Graduate Texts in Mathematics. Springer New York, 2007. ISBN 9780387728315.

[13] Grégoire Ribordy, Jean-Daniel Gautier, Nicolas Gisin, Olivier Guinnard, and Hugo Zbinden. Fast and user-friendly quantum key distribution. *Journal of Modern Optics*, 47(2-3):517–531, Feb 2000. ISSN 1362-3044. doi: 10.1080/09500340008244057.

[14] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. Quantum cryptography. *Rev. Mod. Phys.*, 74:145–195, Mar 2002. doi: 10.1103/RevModPhys.74.145.

[15] Lennart Ljung and Torkel Glad. *Reglerteknik: grundläggande teori*. Studentlitteratur, 4:15 edition, 1981. ISBN 9789144178929.