Photonic Systems Metrology for Quantum Communications Hardware

Sophie Albosh

Doctor of Philosophy

University of York

Physics

December 2021

Abstract

Quantum key distribution (QKD) is a method of sharing encryption keys between parties for the purposes of secure information transfer via public communication channels. QKD systems achieve this by exchanging single photons encoded with the key bit information, where the quantum properties of the optical signals ensures the secrecy of the final key. This is superior to classical key distribution schemes and post-quantum cryptography, as the protocols are not at risk from code-breaking algorithms and advanced computational methods. However, the security of QKD protocols does rely upon the operation and accurate modelling of the hardware used in these systems, to generate and detect the single-photon level signal. To ensure the security of any shared key, the QKD devices must be characterised, where measurements are performed to test and assess the properties of the hardware. Many QKD protocols place requirements on the phase of the optical signals, both for encoding and security purposes.

This work explores the design, construction and initial implementation testing of a measurement system that can be used to characterise the phase properties of QKD transmitter and receiver modules. The system is designed so that it can be used to perform non-intrusive assessments of QKD hardware by sending and measuring optical signals, reducing the risk of any disruption to the device and its performance, which is particularly critical when assessing commercial devices. It is plug-and-play by design, so that it can be easily applied to the assessment of many different devices. It is also portable, so that it can be used to assess QKD hardware in situ.

This work constitutes a step towards providing phase characterisation measurements for QKD hardware, which is necessary to ensure the security of the keys generated via QKD protocols.

Contents

List of Tables

List of Figures

Acknowledgements

This work was conducted at the National Physical Laboratory, Hampton Road, Teddington, Middlesex, TW11 0LW.

I would like to thank the University of York and the National Physical Laboratory for this opportunity. I have thoroughly enjoyed this work throughout the project and I am so grateful for everything I have learned along the way.

I would like to thank Dr Giuseppe Marra for lending his expertise and sharing resources in contribution towards this project. I would also like to thank Dr Robert Starkwood, Dr Philip Dolan, Dr Anthony Vaquero-Stainer, Dr Ke Guo and Luke Arabskyj, for their help and support over the past few years, as well as the support from many other fantastic colleagues at the National Physical Laboratory. My time there would not have been the same without them.

I am truly thankful to my supervisors, Professor Tim Spiller and Dr Christopher Chunnilall, for the many hours of discussion and continued support throughout this project; and also for taking a chance on a theoretical physics graduate, who was a little scared of experiments when first starting this experimental PhD! I couldn't have asked for better supervisors. Thank you.

Finally, I will never be able to quantify how grateful I am for my family and friends who have supported me throughout; I could not have done this without them. Also, to my family, it's been 8 years of higher education, I promise I'll get a job now!

Declaration

I declare that this thesis is a presentation of original work and I am the sole author. This work has not previously been presented for an award at this, or any other, University. All sources are acknowledged as References.

Chapter 1

Introduction

1.1 Cryptography

1.1.1 Encryption and Key Distribution

Cryptography is the practice of securing secret information, so that it simply remains secret. It is implemented in telecommunications to facilitate the secure transfer of information via public communication channels. The process of encryption is employed to keep such information secure, which involves the conversion of the information from a readable form, known as the plaintext, into an unreadable version, known as the cyphertext. To exchange a secret message, the sender will encrypt the information into the cyphertext and send that through a communications channel to the receiver, who will decrypt the information into the plaintext. Here, only the sender and reciever have the ability to perform the encryption and decryption process, so if an eavesdropper accesses the communications channel and copies the information, they will only be able to obtain the unreadable cyphertext, without the means of decrypting it. This encryption and decryption process is enabled by keys, random strings of binary bit values. A key is required to perform encryption and decryption, where these keys should only be known to the sender and receiver. If this is the case, such that the eavesdropper holds no information about the keys, then the message will be kept confidential during the transfer[1].

1.1.2 Security of Encryption Schemes & Quantum Computers

Asymmetric (Public Key) Encryption

There are two categories of encryption schemes, asymmetric and symmetric. In asymmetric encryption, also known as public key encryption[2], different keys are used for the encryption and decryption processes. In public key encryption, the receiver holds both the decryption key and the encryption key and starts by broadcasting the encryption key out to the sender. The sender then uses this encryption key to encrypt their message, which they transmit back to the receiver, who then decrypts it. Here an eavesdropper can obtain the encryption key and the cyphertext, but they cannot obtain the decryption key and therefore they cannot access the plaintext. Examples of public key encryption, schemes include the Rivest Shamir Adleman (RSA) scheme [3] and elliptical curve cryptography (ECC) [4, 5]. The security of public key encryption schemes relies on complex mathematical problems, typically in the form of trapdoor one-way functions. One-way functions are problems that are easy to solve in one direction, but very difficult to solve in the reverse, where for trapdoor one-way functions there exists a piece of information that

[1] A useful introduction to cryptography and encryption can be found here [1].
[2] Originally developed by GCHQ [2]

simplifies the reverse calculation significantly. From the perspective of an eavesdropper, solving such trapdoor one-way functions without the trapdoor information would take a long time using the algorithms and computational technology currently available.

However, new algorithms and improved technology may provide methods for solving the complex mathematical problems, required to decrypt public encryption schemes, much faster than what is currently achievable. For example, RSA relies on prime factorisation, a one-way function [3], which can be solved by Shor's algorithm [6, 7] in polynomial time rather than exponential time, compromising the RSA encryption scheme. Shor's algorithm cannot be performed on traditional computers and instead requires quantum computers that utilise the superposition of quantum systems to perform computational operations. If quantum computers are developed that can successfully run protocols like Shor's algorithm, public key encryption systems will be broken [8] and will no longer be suitable for the prolonged transfer of secret information.

Symmetric (Private Key) Encryption

The other type of encryption scheme is symmetric encryption, where only a single key is used for the encryption and decryption process. Well known symmetric encryption schemes include the Vernam one-time pad (OTP) [9] and the Advanced Encryption Standard developed by NIST [10]. As the keys are the same, prior to encrypting and transmitting secret information, the encryption/decryption key needs to be confidentially shared between the sender and the receiver, which can be achieved using key distribution schemes. Key distribution can be achieved by simple physical means; transferring keys in a locked attaché case, or via communication channels using a public key encryption scheme.

The development of quantum computers poses less of a serious threat to symmetric encryption schemes compared to public key encryption schemes[3]. For example, Grover's algorithm[11], another quantum algorithm, is a database searching algorithm that reduces the security of AES but does not completely break the encryption scheme. Instead AES can continue to be used with adjusted parameters, namely longer lengths of encryption key [8, 12, 13]. However, if a symmetric key encryption scheme relies on public encryption to distribute the keys prior to encryption, the key distribution method may be broken by quantum computers running quantum algorithms.

Quantum-resistant Encryption Systems

The development of quantum computers is an active research field; NIST [8] estimates that a quantum computer capable of breaking 2000-bit RSA will be developed by 2030[4]. Once such a device is constructed, public key encryption systems will be broken and the confidentiality of any information sent via these encryption systems will be compromised. Furthermore, the confidentiality of any information currently sent using these encryption systems is also at risk of being broken in the future. This is because the cyphertexts exchanged now can be recorded and saved by eavesdroppers and decrypted once the encryption system is broken [12]. Therefore it is important to develop, test and implement quantum-resistant encryption systems now, especially when considering confidential information that has a long security shelf-life.

There are two prominent categories of quantum-resistant encryption systems, post-quantum cryptography and quantum key distribution. Post-quantum cryptography is a collection of cryptographic systems that are aimed to be secure from quantum computers,

[3]Note that OTP is information-theoretically secure and therefore will not be affected by the development of quantum computers. However, as OTP does not include a key distribution protocol, the operation of the scheme would require a quantum-secure key distribution method.

[4]Further estimates can be found here [14].

as well as classical computers [5]. These systems provide a feasible solution to the advent of fully functioning quantum computers; however as these protocols continue to base their security in complex mathematical problems, future technological advances and algorithm development may pose a risk to these post-quantum cryptography systems.

Quantum key distribution on the other hand is a collection of key distribution protocols that base their security on the physical properties of quantum systems and are therefore not compromised by classical and quantum computers. In general these systems are not at risk from the same technological and algorithmic developments as post-quantum cryptography and classical cryptography, and as such quantum key distribution protocols can be combined with quantum-resistant symmetric encryption to create secure communications systems.

1.2 Quantum Key Distribution

Quantum key distribution (QKD) protocols consist of encoding binary bit values onto the states of quantum systems, where these quantum systems are then sent from the transmitter to the receiving party, who decode the bit string from the quantum states. The resulting shared bit string can then be processed and used as the encryption/decryption key. There are a wide variety of QKD protocols; they use different encoding states, security measures and quantum systems. There are two particular categories of QKD: discrete variable QKD and continuous variable QKD. Continuous variable QKD uses continuous parameters of the light, such as the quadratures of the electromagnetic field, to encode the bit values of the key[16]. Discrete variable QKD uses a chosen set of discrete states of light, such as polarisation or phase states, to communicate the key. Discrete variable QKD will be the focus of this work.

1.2.1 Phase-encoded BB84 Protocol

BB84 [17] was the the first QKD protocol to be developed and is the basis of many protocols currently researched and is utilised in commercial systems. The protocol involves encoding a bit value (0 or 1) onto the qubit states of single photons, also known as the QKD signal. The photons can be encoded in one of two qubit bases: the Z-basis $\{|0\rangle, |1\rangle\}$ or the X-basis $\{|+\rangle, |-\rangle\}$. Definitions of these qubits and the bases are included in appendix A.1, where the X-basis states are a superposition of the Z-basis states,

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \tag{1.1}$$

$$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \tag{1.2}$$

and, likewise, the Z-basis states are a superposition of the X-basis states,

$$|0\rangle = \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle) \tag{1.3}$$

$$|1\rangle = \frac{1}{\sqrt{2}}(|+\rangle - |-\rangle). \tag{1.4}$$

When measuring the state of an encoded single photon, a measurement basis must be chosen, which collapses the photon state into one of the outcomes pertaining to that basis. This measurement is irreversible and is a property of quantum mechanics; it is not a feature resulting from the measurement apparatus. For example, if a photon is in the state $|+\rangle$ and a measurement is made in the Z-basis, there is a 50% chance of retrieving a state $|0\rangle$

[5] A useful overview of post-quantum cryptography can be found here [15].

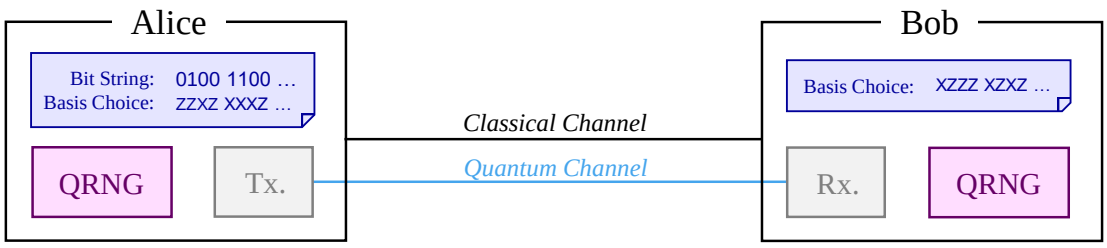


Figure 1.1: The primary elements of a QKD system, consisting of: the sender, Alice, who holds the bit string to send, a quantum random number generator (QRNG) to determine her preparation bases and an optical transmitter (Tx.), and the receiver, Bob, who also holds a QRNG to determine his measurement bases and an optical receiver (Rx.). Alice and Bob are linked via two communication channels, the classical channel and the quantum channel.

and a 50% chance of retrieving a state $|1\rangle$, where this outcome is truly random. The same also applies to the measurement of the state $|-\rangle$ in the Z-basis, or the measurement of either of the Z-basis states in the X-basis. This property of quantum mechanics is critical to the operation of QKD protocols.

The general setup of a QKD system is shown in figure 1.1, consisting of the sender, named Alice, and the receiver, named Bob. Alice and Bob are connected via two channels: a quantum channel that is able to transfer single-photon quantum states between them and an authenticated classical channel[6] used for all other communication signals. Alice and Bob have an optical transmitter and an optical receiver respectively, which are used to prepare, modify and detect the QKD signal. For the phase-encoded BB84 protocol, this involves generating an optical signal and applying phase shifts to create the four qubit states. The details of the structure of the optical transmitter and the optical receiver for the phase-encoded BB84 protocol [17, 19] are shown in figure 1.2. To prepare a qubit, Alice applies a phase shift of ϕ_A to the quantum state, the values of which are detailed in table 1.1. The qubit states of the photons correspond to the applied phase shifts as follows,

$$\begin{aligned} |0\rangle : &\quad \phi_A = 0 \\ |1\rangle : &\quad \phi_A = \pi \\ |+\rangle : &\quad \phi_A = \pi/2 \\ |-\rangle : &\quad \phi_A = 3\pi/2. \end{aligned}$$

Alice and Bob each hold a quantum random number generator (QRNG) that they use to determine which base to respectively prepare and measure the quantum states in[7]. This ensures that Alice and Bob's basis choices are always random and uncorrelated with one another. The operation of the protocol proceeds as follows:

[6] Alice and Bob can authenticate their classical communication channel via authentication protocols, which ensures that they are communicating with one another. Further information on these authentication protocols can be found in [18].

[7] For some QKD protocols a separate QRNG is not needed for this process, however for clarity the presence of a separate QRNG is included here.

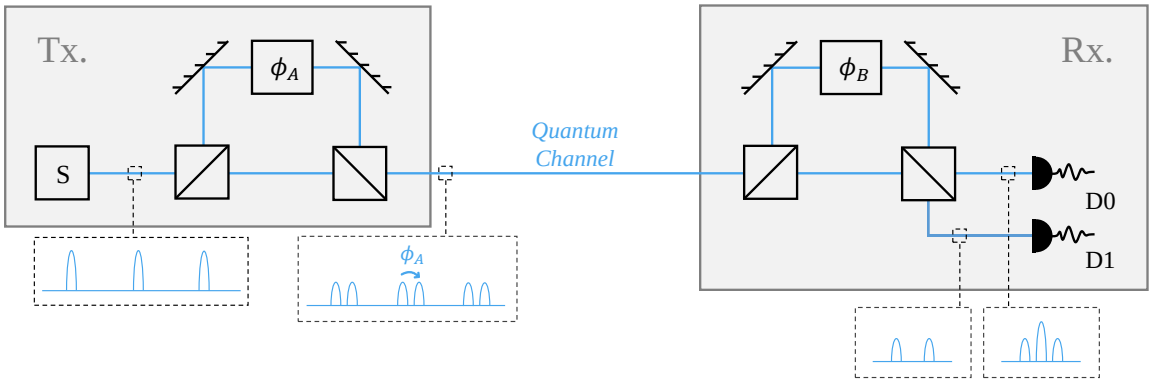


Figure 1.2: Conceptual optical setup of the transmitter (Tx.) and receiver (Rx.) used by Alice and Bob respectively to perform the phase-encoded BB84 protocol. The transmitter consists of a source (S) and an asymmetric Mach-Zehnder interferometer (comprising two beam splitters and two mirrors) with a phase shifter (ϕ_A). The source is either a single-photon source or a highly attenuated pulsed laser. The receiver consists of a matched asymmetric Mach-Zehnder interferometer with a phase shifter (ϕ_B) and two single-photon detectors (D0 and D1). For a source producing optical pulses, the pulse diagrams (dashed boxes) indicate the state of the optical signal at different stages within the setup.

Alice's Phase Shift (ϕ_A)

Basis	**Bit 0**	**Bit 1**
Z	0	π
X	$\pi/2$	$3\pi/2$

Bob's Phase Shift (ϕ_B)

Basis	ϕ_B
Z	0
X	$\pi/2$

Table 1.1: Phase shifts performed by Alice and Bob in the phase-encoded BB84 protocol. The value of ϕ_A is dependent on the preparation basis selected by Alice and the value of the key bit to be sent. The value of ϕ_B is dependent only on the measurement basis selected by Bob.

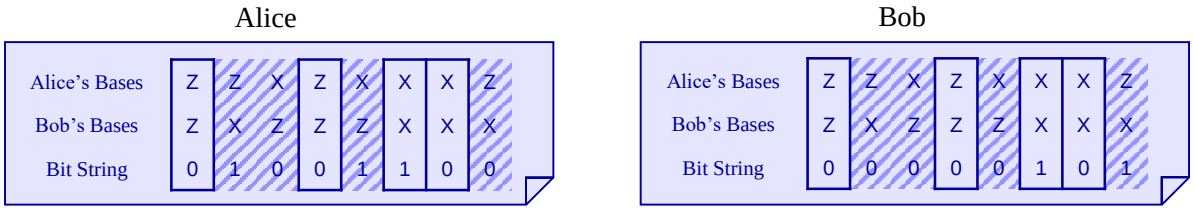


Figure 1.3: Depiction of basis reconciliation performed by Alice and Bob to distil the key from the shared bit string in the BB84 protocol. If Alice and Bob use the same basis to prepare and measure the quantum state, they keep the bit value. If Alice and Bob use different bases to prepare and measure the quantum state, they discard the bit value (crossed out).

Phase-encoded BB84 Protocol

1. Alice selects a single bit of the bit string and uses the QRNG to determine the preparation basis. She uses the encoding table 1.1 to determine what phase shift, ϕ_A, to apply to the quantum state. Alice records the basis and the bit value, prepares the quantum state and sends it to Bob via the quantum channel.

2. Bob uses a QRNG to determine his measurement basis and makes a record of the chosen basis. He measures the quantum state sent from Alice, where he applies a phase shift ϕ_B according to table 1.1. If detector D0 clicks, he records a bit value of 0, if detector D1 clicks he records a bit value of 1.

3. Steps 1 and 2 are repeated for every bit in the bit string that Alice holds.

4. After all bit values have been exchanged Alice and Bob perform basis reconciliation, where they compare the bases they used for every round. Alice and Bob then perform sifting; for all rounds where they have used the same basis they keep the bit, whereas if they have used different bases, they discard the bit. These processes are depicted in figure 1.3.

5. To distil a secure key from the shared bit string, Alice and Bob perform error correction and privacy amplification procedures to correct for experimental imperfections and any issues caused by potential eavesdroppers [20]. Depending on the conditions during the photon exchange, it may not always be possible to extract a secure key from the bit string.

The basis reconciliation process is performed via the classical communications channel, where the basis information can be made public after the bit exchange without compromising the security of the final key. When Alice and Bob pick the same basis, assuming no experimental error and no eavesdropper interference, there is a 100% chance Bob will record the same value as Alice. However, when Alice and Bob pick different bases, there is only a 50% probability of Bob recording the same bit value that Alice sent[8]. By discarding all rounds where Alice and Bob choose different bases, they discard approximately half of their shared bit string, however the resulting string they share is the same, apart from experimental and eavesdropper-related errors. After performing key distillation procedures, the shared bit string between Alice and Bob can then be used as a key. For OTP, once this key is used to encrypt and decrypt information it should be discarded.

1.2.2 Security of QKD Protocols Against Eavesdroppers

As stated previously, QKD protocols base their security on the physical properties of the quantum systems. In the case of the phase-encoded BB84 protocol, these quantum states are the single photons that are transmitted from Alice to Bob. If an eavesdropper, named Eve, attempts to gain information about the key by attacking the quantum channel, she will have to interact with these photons directly, which will have an impact on the quantum state of the photon as dictated by quantum mechanics. This is the unique security feature of QKD systems that is not present in other classical cryptographic protocols. Of course Eve can choose to attack other elements of the QKD systems, as with any other classical cryptographic system, such as schemes targeting the transmitter/receiver or more simple denial of service attacks. These types of attack can be defended by implementing physical and procedural countermeasures, which are discussed further in section 1.3.

[8]Here it is assumed that Alice and Bob use both bases for bit encoding and that they pick these bases with equal probability. This is not necessarily the case for all QKD protocols.

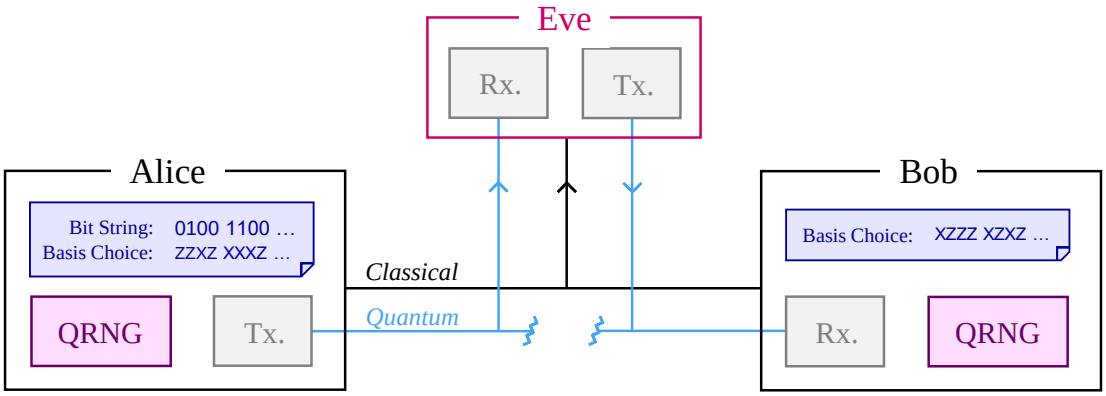


Figure 1.4: Diagram of the intercept-resend attack [17]. Alice and Bob hold a transmitter (Tx.) and a receiver (Rx.) respectively and a QRNG each. Eve has severed the quantum channel and coupled it to her own transmitter and receiver. Eve can also listen and copy any information sent through the classical communication channel.

To demonstrate the unique quantum-based security feature of QKD, it is useful to consider an eavesdropping attack named the intercept-resend attack [17] performed against the BB84 protocol. In this attack, Eve severs the quantum channel between Alice and Bob and connects the quantum channel to her own transmitter and receiver pair, as shown in figure 1.4. For each photon that Alice sends during the BB84 protocol, Eve chooses either the Z- or X-basis to measure the photon state and then recreates the state she measured in that same basis. After recreating the state, she sends it to Bob, and repeats this for every bit in the bit string. As Eve cannot predict the bases that Alice uses, she cannot match her detection and preparation base to that of Alice's. Therefore, assuming that she chooses her bases at random with equal probability, then she will match bases with Alice on around half of the photon exchanges. When Alice and Eve's basis choices match, Eve will be able to successfully recreate the state that Alice sent, and will therefore be able to learn the bit value that Alice is sending[9]. However, if Alice and Eve's basis choices differ, Eve will prepare a state in the wrong basis and will only have a 50% chance of determining the correct bit value for a bit which Alice and Bob agree to keep.

As is clear, when Eve chooses a different basis to Alice, she sends a state to Bob in the wrong basis, resulting in a 50% chance of Bob recording the wrong bit value. A summary of all of the outcomes depending on the basis choices made by Alice, Bob and Eve are shown in figure 1.5. When Alice transmits many bits to Bob, this mismatch of bases between Eve and Alice results in errors in the bit string shared by Alice and Bob after basis reconciliation. For example, if Eve picks her bases at random with equal probability, her interference will result in $\sim 25\%$ of the bit string being incorrect. Alice and Bob can determine the proportion of errors in the bit string they share; the simplest method of doing this is to sacrifice a small portion of the string and compare the bit values publicly [17]. The proportion of errors in the bit string can be used to determine the maximum amount of information that Eve may hold about the bit string and therefore the final key, depending on the protocol and the privacy amplification procedures. If the proportion of errors exceeds a set threshold, then a secure key can no longer be distilled from the bit string. When this happens, Alice and Bob discard the bit string and restart the protocol.

QKD systems are not resistant to denial of service attacks; if only a single quantum and classical communication channel link Alice and Bob, Eve can easily sever that line

[9]It is assumed that Eve has access to information about the classical elements of the QKD system, such that she can determine the bit value corresponding to the qubit state she measures.

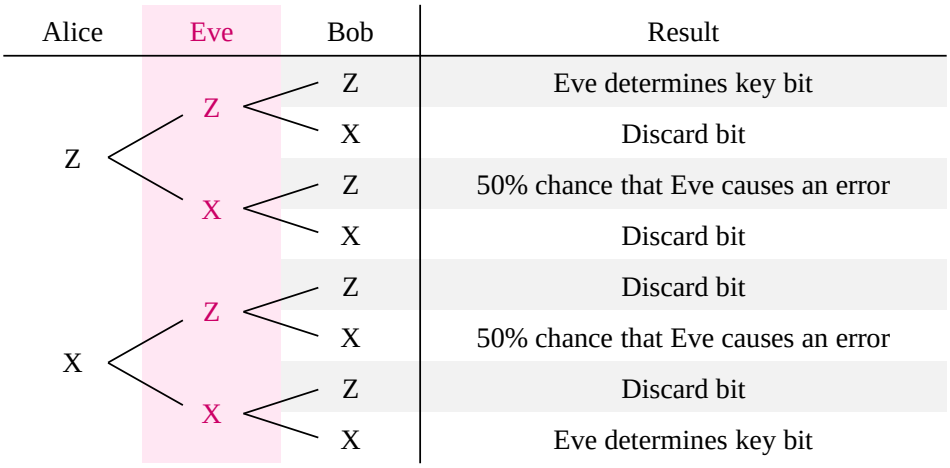


Figure 1.5: Diagram detailing the possible outcomes for each bit value sent when an intercept-resend attack is performed by Eve on the BB84 protocol. The outcomes for every combination of basis choices made by Alice, Eve and Bob are shown. For each bit value sent, there is a 25% chance that Eve causes an error in Alice and Bob's shared bit string.

or disturb the quantum channel to such an extent that no key can be distilled. However, assuming that Eve's aim is to access the secret information that Alice and Bob are going to encrypt and exchange using the shared key, Eve will want to determine the key without Alice and Bob's knowledge. If she is able to accomplish this, Eve will be able to decrypt the cyphertext as it is passed from Alice to Bob using the key that she has stolen during the key distribution stage. In this way, QKD ensures the security of the information, as Alice and Bob can predict the amount of information Eve has about the key, and can therefore determine if it is compromised. If they decide that the key is compromised, they simply discard it, and do not risk sending the secret message with an unsafe key.

1.2.3 QKD Transmitters & Receivers

The primary elements to any QKD system are the transmitter and receiver held by Alice and Bob. The transmitter must be able to prepare a quantum system in the state that Alice intends to send and the receiver must be able to accurately detect this state, so that Bob can determine the bit value. However, as quantum systems usually consist of a few particles or less, these tasks are difficult to accomplish and require highly technical, sensitive hardware. Developing this hardware is an ongoing research field and producing commercial devices is expensive and therefore an important factor when considering commercial implementation of QKD systems.

Single-photon Sources and Attenuated Laser Sources

Ideally for most discrete variable QKD protocols, the quantum systems used to transmit the key are single photons. For each element of the bit string, Alice encodes the bit value onto the state of a single photon and sends it to Bob, who detects the photon and determines its state. To achieve this, Alice must hold a single-photon source that is able to generate a single photon on demand, where for communications the rate of single photon generation will be on the order of GHz. Useful reviews of current sources for single-photon generation can be found in [21, 22], where these methods, although feasible, can be difficult to realise in QKD experiments [23].

An alternative optical source that is used in many QKD systems is an attenuated

pulsed laser, which produces a very weak intensity pulse in a specific optical mode as a substitute to a single photon. Laser light can be represented quantum mechanically as a coherent state [24]

$$|\alpha\rangle = e^{-|\alpha|^2/2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle \tag{1.5}$$

which is a superposition of the Fock states $|n\rangle$ of the optical mode, with probability coefficients parametrised by the complex variable α. Applying a phase shift of θ to this laser light can be simply represented by a coherent state in the following transformation $|\alpha\rangle \rightarrow |\alpha e^{i\theta}\rangle$. To resemble the desired single photon states needed for QKD, the coherent state of the laser light can be phase randomised ($\theta \in [0, 2\pi)$) resulting in the state:

$$\frac{1}{2\pi} \int_0^{2\pi} |\alpha e^{i\theta}\rangle \langle \alpha e^{i\theta}| \, d\theta = e^{-|\alpha|^2} \sum_n \frac{(|\alpha|^2)^n}{n!} |n\rangle \langle n| \, . \tag{1.6}$$

This phase randomisation is a requirement of the security proofs of the BB84 protocol, as any remaining phase correlations can pose a risk to the security of the key [25]. The resulting expression is a mixture of independent Fock states, where the photon number of the state n follows a Poissonian distribution, with the mean photon number of the distribution given by $|\alpha|^2$. Therefore the probability of having m photons in a phase randomised coherent state is given by,

$$p_m = \langle m| \left[e^{-|\alpha|^2} \sum_n \frac{(|\alpha|^2)^n}{n!} |n\rangle \langle n| \right] |m\rangle = e^{-|\alpha|^2} \frac{\left(|\alpha|^2\right)^m}{m!}. \tag{1.7}$$

In a QKD system these coherent laser light states can be generated and converted into low intensity pulses, where one of these pulses is used to encode and transmit a single bit of the key. Generating laser light, converting it into pulses and attenuating this light down to low intensity can be easily accomplished with commercial devices and pulse repetition rates ≥ 1 GHz are achievable. Therefore using a weak laser source is currently the preferable option compared to using single photon sources in commercial and research-based QKD systems. However, as shown by equation 1.6, the state is a mixture of independent Fock states with photon number n. This means that one of the three following situations can occur:

- 0 photons in a pulse with probability $p_0 = e^{-|\alpha|^2}$
  If the laser pulse contains no photons then no bit information can be transferred from Alice to Bob.
- 1 photon in a pulse with probability $p_1 = |\alpha|^2 e^{-|\alpha|^2}$
  This is the ideal situation that resembles a single photon state, only 1 photon is encoded with the bit value information and therefore this information can be transferred from Alice to Bob.
- > 1 photons in a pulse with probability $p_{>1} = 1 - \left(1 + |\alpha|^2\right) e^{-|\alpha|^2}$
  All photons in the pulse will be encoded with the bit information, therefore the bit information can be transferred from Alice to Bob. However, as multiple photons are encoded there exists redundancy, which poses a security risk.

To reduce the likelihood of more than 1 photon being produced and therefore encoded with the same bit information, the mean photon number of the laser light $|\alpha|^2$ is reduced significantly. In practice a mean photon number of $|\alpha|^2 = 0.1$ is a reasonable setting, which results in probabilities of $p_0 = 90.48\%$, $p_1 = 9.05\%$ and $p_{>1} = 0.47\%$. Although successful

in significantly decreasing the probability of encoding redundancy, reducing the mean photon number lowers the efficiency of the QKD protocol significantly as, in this case, less than 10% of the encoded systems are able to successfully transfer the bit information from Alice to Bob. There are procedures that can be implemented to avoid this issue when using attenuated laser pulses for the QKD signal, namely the decoy state method [26–28]. This generally involves Alice transmitting non-encoding pulses that typically have a higher or lower intensity than encoding pulses, where the yield of encoding to decoy pulses detected by Bob can be used to evaluate the actions of an Eavesdropper.

Single-photon Detectors

Single-photon detectors are devices used to detect the presence of a single photon. They can be either photon number resolving, where they are able to determine whether there is more than one photon present, or non-photon number resolving, where they are not able to determine the difference between the presence of one photon and more than one photon. Photon-number resolving detectors are still relatively rare and relatively undeveloped. However, QKD systems typically only require the use of non-photon number resolving detectors, where there is a range of approaches to performing single-photon detection. The two most prevalent methods of single-photon detection are via the use of single-photon avalanche photodiodes and superconducting nanowire single-photon detectors. Single photon avalanche diodes are a pn-junction that is operated in reverse Geiger mode, where the absorption of a single-photon in the active area results in the creation of an electron-hole pair, which in turn generates an avalanche of secondary charge carriers leading to a detectable electrical response. Superconducting nanowire single-photon detectors consist of a cooled superconducting wire carrying a current, such that the wire is near its critical current density. The absorption of a photon onto the wire results in local heating, which causes the current to surpass the critical value. This results in the wire's resistance changing from superconduction to a normal level, generating a detectable electrical signal. Reviews of these and other single-photon detection techniques can be found in [21, 22].

1.2.4 Overview of Phase-based QKD Protocols

Although there are a variety of different optical parameters that can be used to encode the bit values of a key, phase-encoding is utilised by many different fibre-based QKD protocols. In addition, protocols also place security-based requirements on the phase properties of the optical signal used. The following provides a brief overview of a selection of QKD protocols that, in addition to phase-encoded BB84, utilise phase[10].

Coherent One Way

The coherent one-way (COW) protocol [29] uses time-bin encoding to exchange the bit values. Alice generates a train of coherent pairs of pulses, where each pair encodes one key bit value and the temporal position of the first and second pulse is denoted by t_1 and t_2 respectively. To encode a bit value of 0, Alice places a pulse at t_1 but leaves t_2 empty. To encode a bit value of 1, Alice places a pulse at t_2 but leaves t_1 empty. To ensure the security of the protocol, Alice also sends decoy states, where she places a pulse at t_1 and t_2. These decoy states are not used to encode bit values. Bob's receiver setup consists of an unbalanced coupler that splits the incoming signal from Alice and sends it towards two sets of detectors. The first detector is used to determine the time of arrival of the pulses, allowing Bob to decode the bit values. The second set of detectors performs a

[10]This is not an exhaustive list.

phase measurement between pulses to check the coherence of the incoming pulses, which ensures the security of the protocol.

Differential Phase Shift & Related

The differential-phase-shift (DPS) protocol [30] involves generating a train of pulses, where Alice phase-modulates every pulse by $\{0, \pi\}$ to encode the bit values and Bob measures the phase difference between each of the pulses to determine these values. If an eavesdropper attempts to perform an intercept-resend attack, as the average photon number per pulse is < 1, Eve will not always be able to determine the bit value, and will therefore send a signal with phase encodings different to Alice, resulting in errors. An advancement to the DPS protocol is the differential-quadrature-phase-shift (DQPS) protocol [31], which also generates a train of coherent pulses with a mean photon number per pulse < 1. Each pulse is phase modulated by either $\{0, \pi\}$ or $\{\pi/2, 3\pi/2\}$ to perform the phase encodings and Bob determines the bit value by measuring the pulses and applying a phase shift of $\{0, \pi/2\}$. The round-robin differential phase shift (RRDPS) protocol [32], similar to DPS, applies phase shifts to pulses in a pulse train of $\{0, \pi\}$ to encode the bit values. However in addition to this, the signal is split into separate sets of pulse trains, where the phase is randomised between each set.

Measurement Device Independent QKD

Measurement device independent QKD (MDI-QKD) [33] consists of three parties Alice and Bob, who are both transmitters, and Charlie an untrusted receiver. To execute the protocol Alice and Bob each prepare phase-randomised pulses in one of four polarisation states, where each of these polarisation states correspond to the qubit encodings of BB84, $\{|0\rangle, |1\rangle\}$ and $\{|+\rangle, |-\rangle\}$. Alice and Bob then send each of these states to Charlie, who performs a Bell state measurement and relays his results to Alice and Bob via a public channel. Alice and Bob can then use this information to distil a key.

Twin-field QKD

The twin-field QKD (TF-QKD) protocol [34], bears similarities with MDI-QKD, but allows for key distribution over longer distances and improves on the achievable key rate. The protocol also consists of three parties, Alice and Bob, who are both transmitters, and Charlie an untrusted receiver. Alice and Bob prepare pulses that are both phase encoded and phase randomised. The pulses are then sent to Charlie who interferes them and relays his results to Alice and Bob. From this Alice and Bob distil a key.

Overview of Protocols & their Phase Requirements

Table 1.2 provides a summary of the phase-based requirements of the selection of QKD protocols noted above.

1.2.5 Implementation of Phase Randomisation

Some of the QKD protocols mentioned in the previous section are required to have some element of phase randomisation between pulses or sets of pulses. For example, in a realistic scenario, the operation of phase-encoded BB84 will involve the use of attenuated laser pulses instead of single photons and will incorporate the decoy state method [26–28] to improve the key rate. Here it is required that the phase between the encoding pulse pairs is completely randomised [27, 35]. However, achieving complete continuous phase randomisation in a physical setup is not straightforward and also difficult to verify [36].

QKD Protocol	**Phase Encoding**	**Details & Other Phase-based Requirements**
Phase-encoded BB84 [17]	✓	Phase encodings of $\{0, \pi/2, \pi, 3\pi/2\}$. Phase randomisation between pulses belonging to different qubit pairs.
COW [29]	✗	All pulses must be coherent (phase difference = 0).
DPS [30]	✓	Phase encodings of $\{0, \pi\}$
DQPS [31]	✓	Phase encodings of $\{0, \pi/2, \pi, 3\pi/2\}$
RRDPS [32]	✓	Phase encodings of $\{0, \pi\}$. Phase randomisation between pulse train sets.
MDI-QKD [33]	✗	Phase randomisation between pulses.
TF-QKD [34]	✓	Phase encoding and phase randomisation between pulses.

Table 1.2: Summary of the phase-based requirements of a selection of QKD protocols.

There are two methods of achieving phase randomisation, via either passive or active means. Passive phase randomisation involves switching the laser off between pulse generations where, if the laser cavity is empty before lasing, the generated laser light results from spontaneous emission. This results in the phase of the generated light being completely random [37]. However, if the cavity is not empty and photons from a previous lasing event are present, the phase of any generated light may be correlated to that produced previously; the phase between generated pulses will not be random. For the laser cavity to be empty, sufficient time must be given to allow all photons from any previous lasing to decay, which may be difficult to achieve when performing QKD protocols at the high clock rates required for telecommunications [36–38].

The active method of phase randomisation involves utilising a phase modulator and a QRNG to apply random phase shifts to the optical pulses. However, it is not feasible to apply one random phase shift chosen from an infinite number of possible phase values in the range of $[0, 2\pi)$ using this method. Alternatively, one can apply a random phase shift selected from a discrete number of phases, where it has been shown that a set of ten different phases provides key rates similar to that of a continuous phase set [36].

The TF-QKD protocol already incorporates the idea of discrete phase randomisation into the protocol through the use of phase slices; the phase range $[0, 2\pi)$ is split into sections where the random phase shifts applied fall into one of these sections [34].

1.3 Eavesdropping, Countermeasures and Characterisation

1.3.1 Eavesdropping & Countermeasures

Given the single-photon nature of the QKD signal, the signal itself is inherently protected from eavesdropping attacks due to the nature of quantum mechanics. To prove the security of a QKD protocol, there should exist a theoretical description of the system known as

the security proof, which outlines the operation of the protocol, the amount of privacy amplification required and any assumptions made about the physical system that must be met in order to distil a secure key. These security proofs of protocols can be grouped into three classes, which are security against individual attacks, collective attacks and coherent attacks [23]. In individual attacks, Eve is only able to perform individual distinct measurements on each photon in the QKD signal, and therefore security against individual attacks makes assumptions about the capabilities of the eavesdropper and is the weakest form of security of a protocol. Alternatively, coherent attacks only require that Eve obeys quantum mechanics, and therefore she can perform joint measurements on the all of the photons contained within the QKD signal. Therefore security against coherent attacks provides the strongest form of security and makes no assumptions about Eve's capabilities. Collective attacks are an intermediate between the two, placing some assumptions on what Eve can accomplish experimentally [23].

These attacks all focus on Eve targeting the QKD signal however, Eve is able to perform more complex attacks targetting the transmitter and receiver devices held by Alice and Bob. These types of attacks are known as side-channel attacks, where Eve aims to extract information about the key from any elements of the devices held by Alice and Bob via whatever means possible. For example, a Trojan-horse attack [39] is where Eve sends a probe optical signal through the quantum channel to Alice's transmitter. Eve can then measure any back-reflections of her probe signal or perform other complex techniques to extract information about Alice's devices, for example any imparted phase shifts, which can inform Eve about the key bit values. To ensure the security of a QKD protocol, these types of attacks must be countered.

To ensure the security of a QKD system in the presence of side-channel attacks, countermeasures can be incorporated into the security proof of a protocol. These countermeasures typically involve including extra steps in the experimental procedure to subvert the attack or introducing new hardware to detect the presence of an attack. For example, for the Trojan-horse attack Alice can choose to couple a detector into the quantum channel at her transmitter output to detect the presence of a probe signal sent by Eve [40]. Once these requirements are implemented into the security proofs, it is vital that the experimental realisations of a protocol fulfil the assumptions made by the proof for the security of the generated key. To ensure that a physical QKD system is compliant with these assumptions, it is necessary to characterise the devices.

1.3.2 Characterisation

Characterisation of QKD hardware allows the potential information leakage to an eavesdropper to be quantified. This is a necessary step to ensure the implementation security of a QKD system [20] thereby ensuring the security of any generated key. A characterisation measurement involves experimentally measuring the properties of a device, which can concern any aspect of the hardware. For QKD devices this could include, but is not limited to,

- The mean photon number per pulse of the output signal
- The phase properties of the output signal or the phase shifts performed inside the devices
- The polarisation of the output light to ensure there is no redundant encoding
- Properties of the single-photon detectors in the receiver or the functionality of any monitoring sensors

Procedures for characterising the individual components of a QKD system have been specified [41], for example the components of a transmitter or receiver device. Furthermore, there is currently work within standards organisations, such as ISO/IEC and ETSI to develop characterisation procedures for complete QKD modules [42–44]. Here a QKD module refers to a whole transmitter or receiver device.

When devising a characterisation measurement procedure for these modules, the aim is to perform nonintrusive tests that minimise any disturbance to the hardware. This is to avoid any alteration or damage to the device which may compromise its functionality or generate new side-channels that could be attacked by an eavesdropper, both of which could compromise the security of any generated keys. This approach also benefits the analysis of commercial devices, where customer warranty may be infringed or revoked if, for example, the device is opened as a result of an intrusive test procedure.

1.4 Phase Characterisation & Project Summary

Given the prevalence of phase-encoded QKD protocols and the extra requirements placed on the phase of the QKD signal, it is critical that the hardware used in QKD systems applies and manipulates the phase of light accurately and in line with the assumptions made by the security proof. This particularly concerns the transmitter, which must be able to generate a QKD signal with the correct phase encodings where necessary and/or provide phase randomisation or coherence between pulses within the pulse train. Additionally, where required the receiver must also perform accurate phase shifts, for example in phase-encoded BB84 where this phase shift determines the measurement basis. It is therefore necessary to characterise the phase properties of QKD hardware, to ensure the security of the generated key for all protocols that place requirements on the phase of the QKD signal, which is the focus of this work. No standards, either published or in draft, address detailed procedures for characterising these properties[11] [45].

1.4.1 Project Summary

The project work concerns the design, construction and application of a measurement system that can be used to characterise the phase properties and settings of QKD devices. The measurement system should be able to perform characterisations of both transmitter and receiver modules and where possible treat these devices as black boxes. The measurements performed should be nonintrusive, avoiding mechanically opening QKD modules and minimising any disturbance to the devices. To achieve this, the measurement system will focus on the assessment of optical signals to perform phase characterisation procedures.

The measurement system will be based around an asymmetric Mach-Zehnder interferometer (AMZI), which can be combined with other devices, such as optical sources and single-photon detectors to perform phase measurements. The system should be:

1. Able to characterise the phase shifts applied by transmitter and receiver modules to the QKD signal

2. Able to distinguish between cases of consistent phase application and phase randomisation

3. Plug-and-play in design, so that it can be easily applied to many different QKD devices

[11] ISO/IEC 23837-2 (in draft) states the requirement for measuring the phase of transmitted states using appropriate instrumentation, but no detailed measurement procedures are specified.

4. Transportable so that it can be used to characterise QKD devices in situ

Depending on the design of the measurement system, it may also have further application in other characterisation procedures.

The structure of this thesis is as follows. Chapter 2 explores the relevant phase measurement theory to aid in the design of the system. Chapter 3 details the measurement system design and construction, as well as preliminary testing and development of characterisation procedure. Chapter 4 concerns the assessment of laser source using the measurement system, as well as a pseudo QKD transmitter signal, detailing the characterisation procedure. Chapter 5 explores the characterisation of a prototype QKD device, which is used to demonstrate the functionality of the measurement system when applied in test procedures designed to assess both transmitter and receiver QKD modules. Finally, chapter 6 discusses the conclusions and highlights potential future work.

Chapter 2

Phase Measurement Theory and Preliminary Testing

2.1 Phase Measurements for Characterisation

The security of a key generated via a QKD protocol is dependent on the performance and the correct operation of the hardware used in the QKD system. QKD transmitters must generate light pulses with the specific properties described in the associated protocol and security proof, which typically impose requirements on the phase of the QKD signal. To test whether a QKD transmitter is producing an optical signal with the correct phase properties, the transmitter must be characterised, where the method used to characterise the device can take various forms. As detailed in section 1.3.2, in the assessment of QKD modules it is beneficial to avoid intrusive measurements that require opening or disturbing the device. It is favourable instead to assess the phase properties of these devices by measuring optical signals, where in the case of a transmitter, this would involve measuring the QKD signal directly. This approach also directly results in the development of a versatile characterisation method that can be applied to almost all QKD devices, including receiver modules.

The pulses of light emitted from a QKD transmitter form a pulse train, where typically each pair of pulses is used to encode one bit of the key[1]. To measure the phase difference between two chosen pulses in the train, the pulses can be overlapped with one another using an asymmetric Mach-Zehnder interferometer (AMZI), where the delay between the arms is equivalent to the temporal separation of the chosen pulses. See figure 2.1. At the second beam splitter of the AMZI the pulses interfere, where the phase difference between the pulses determines the proportion of light exiting each of the two outputs. The temporal delay of the AMZI can be adjusted to overlap any two chosen pulses within the pulse train. In QKD systems, the phase difference between pulses that correspond to the same encoding qubit is known as the local phase (ϕ_L) and the phase difference between pulses that belong to different encoding qubits is known as the global phase (ϕ_G). It is important to assess both the local and global phase within the pulse train from the transmitter, as QKD protocols may set requirements on the values of these phase differences, see section 1.2.4 for further details.

If the pulses of light emitted from the transmitter are bright (containing many photons), the phase difference between two pulses can be determined by measuring those two pulses alone. When a bright pulse is sent into the AMZI, the pulse is initially split at the first beam splitter, where some of the light travels down one arm of the interferometer and the rest of the light travels down the other. This creates two pulses that are temporally

[1]For the BB84 protocol, each pair of pulses may originate from a single laser pulse that has propagated through an AMZI.

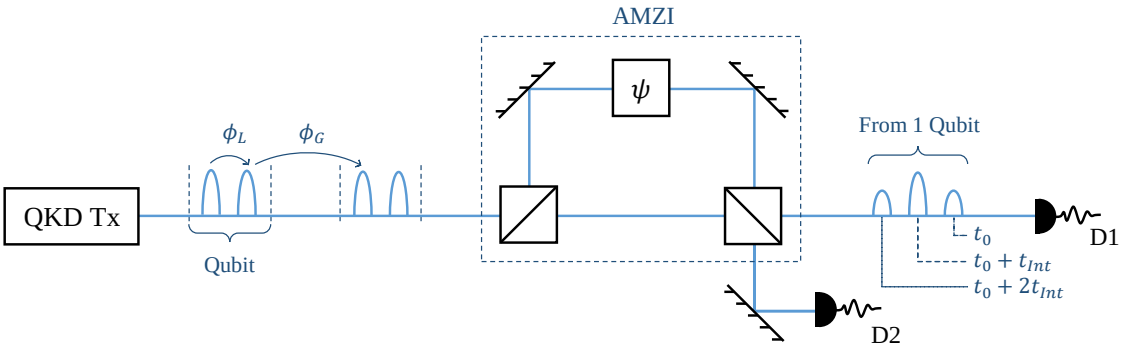


Figure 2.1: A simple schematic of a measurement system that could be used to perform the phase characterisation of a QKD transmitter (QKD Tx). The system consists of an asymmetric Mach-Zehnder interferometer (AMZI) and detectors (D1, D2). The AMZI has a temporal delay between the two arms of t_{Int} and consists of two unpolarised 50:50 beam splitters (box with diagonal line) and a phase shifter that imparts a phase difference of ψ between pulses that propagate down opposite arms of the interferometer. The local phase (ϕ_L) is the phase difference between pulses corresponding to the same qubit and the global phase (ϕ_G) is the phase difference between pulses corresponding to different qubits. Note that the global phase can refer to the phase difference between any two pulses in the train that don't correspond to the same qubit.

separated by the time delay of the interferometer t_{Int}. If two pulses that are separated by t_{Int} are sent into the interferometer, there will be three output pulses of light, as shown in figure 2.1. The pulse at t_0 results from the first pulse travelling through the short arm of the AMZI and the pulse at $t_0 + 2t_{Int}$ results from the second pulse travelling through the long arm of the AMZI. The centre pulse at $t_0 + t_{Int}$ is a combination of the first pulse having travelled through the long arm and the second pulse travelling through the short arm, resulting in their overlap and interference. For this centre pulse, the phase difference between the pulses determines the proportion of light that exits the AMZI towards detector D1 and D2. Equations for the optical power measured at both detectors for the pulse at $t_0 + t_{Int}$ are given by,

$$P_1 = \frac{1}{2} P_0 \eta_1 \left[1 - \cos(\phi + \psi)\right] \tag{2.1}$$

$$P_2 = \frac{1}{2} P_0 \eta_2 \left[1 + \cos(\phi + \psi)\right] \tag{2.2}$$

where P_0 is the input power, η_1 (η_2) is the detection efficiency of detector D1 (D2), ϕ is the encoded phase difference between the initial pulses and ψ is the phase difference imparted between the pulses by the AMZI. Varying the value of ψ between 0 and 2π will result in the output optical power changing, producing an interference pattern as shown in figure 2.2. The power detected at either D1 or D2 can be used to calculate the phase difference between the emitted pulses.

However, as the pulses from a QKD transmitter are at the single-photon level (typically < 1 photon per pulse) the phase difference between a pair of pulses cannot be determined by measuring those pulses alone. This is because a photon approaching the final beam splitter cannot be shared and detected at both D1 and D2, and therefore cannot indicate the proportion of light sent towards each detector. Instead the probability of the photon exiting towards D1 or D2 is determined by the phase difference of the two interfering

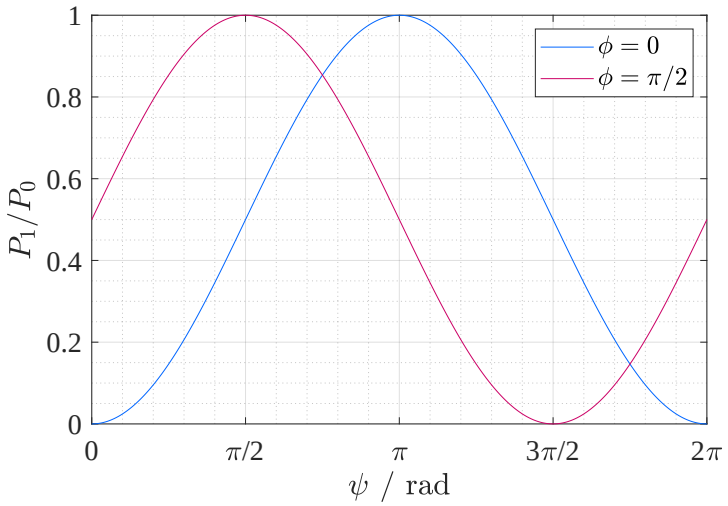


Figure 2.2: Interference patterns for varying the AMZI phase ψ, calculated using equation 2.1 with $\eta_1 = 1$, equivalent to 100% detection efficiency. The patterns for two values of pulse phase differences ϕ are shown.

pulses. For QKD pulses, D1 and D2 are single-photon detectors (SPD) that can detect the presence of one or more photons, resulting in a detector click, or no photons, resulting in no-click. For perfect SPDs the probability of the detectors registering a photon is given by,

$$p_{1-click} = \frac{1}{2}\left(1 - \cos(\phi + \psi)\right) \tag{2.3}$$

$$p_{2-click} = \frac{1}{2}\left(1 + \cos(\phi + \psi)\right) \tag{2.4}$$

where ϕ and ψ are the same as described previously. Therefore to determine the phase difference between single-photon pulses at a chosen separation, many pairs of those pulses must be measured. Each pair of pulses measured will be registered as a click at either detector D1 or D2, where after many measurements the phase difference may be determined. It should be noted that to successfully characterise a single phase setting of the QKD transmitter, the phase difference between the pulses being measured at a specific temporal separation must be consistent over the measurement duration.

To successfully perform the desired phase characterisation measurement, the simple measurement system model represented in figure 2.1 is further developed. The features of the model will inform the design and construction of the measurement system, as well as the characterisation procedures it performs.

2.2 Measurement System Components

In the following a model for the measurement system is developed, exploring components and techniques used in the system and assessing the errors associated with any procedures required as part of the phase characterisation process. Initially the individual components of the system are modelled, which are then combined to create a full model of the measurement system.

2.2.1 Coherent Laser Pulses

The model will focus on the use of weak laser pulses for the QKD signal, rather than a single-photon signal, given the prevalence of weak coherent sources in QKD systems.

However, it should be noted that the measurement system can also be used to assess QKD devices that operate with single-photon signals or employ single-photon sources. Coherent states can be used to represent laser light, where a coherent state is defined [24],

$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle \qquad \text{(1.5, revisited)}$$

which is a superposition of Fock states, $|n\rangle$. Fock states are the eigenstates of the number operator $\hat{N}$, $\hat{N}|n\rangle = n|n\rangle$, where n is the number of photons in that state [46]. The complex parameter α defines the phase properties of the coherent state and the average photon number, which is given by $\mu = |\alpha|^2$ [24] and is proportional to the optical power of the signal (P_0). This coherent state represents continuous wave (CW) laser light; to model pulses of laser light, temporal modulation must be included. Taking the laser pulse shape to be Gaussian, the k^{th} pulse in a pulse train can represented as the following coherent state [47],

$$|G_k \alpha_k\rangle = e^{-{G_k}^2 |\alpha_k|^2/2} \sum_{n=0}^{\infty} \frac{(G_k \alpha_k)^n}{\sqrt{n!}} |n\rangle \tag{2.5}$$

where,

$$G_k = \left(\frac{4\ln(2)}{\pi \tau_k^2}\right)^{\frac{1}{4}} e^{-2\ln(2)(t-\delta_k)^2/\tau_k^2} \tag{2.6}$$

G_k^2 is a Gaussian distribution, τ_k is the full width half maximum of the pulse duration, t is time and δ_k is the time at the peak of pulse k. See appendix B.1.1 for the derivation. The resulting mean photon number of the laser pulse is given by [47],

$$\mu_k = \int_{-\infty}^{\infty} \left| G_k \alpha_k e^{i\phi_k} \right|^2 dt = |\alpha_k|^2 \tag{2.7}$$

the derivation of which is shown in appendix B.1.2. To incorporate the phase differences between pulses, the phase shift operator is introduced [46],

$$\hat{P}_k = e^{-i\phi_k \hat{N}} \tag{2.8}$$

where ϕ_k is the applied phase shift and

$$\hat{P}_k |G_k \alpha_k\rangle = |G_k \alpha_k e^{-i\phi_k}\rangle \,. \tag{2.9}$$

The final state,

$$|G_k \alpha_k e^{-i\phi_k}\rangle = e^{-{G_k}^2 |\alpha_k|^2/2} \sum_{n=0}^{\infty} \frac{\left(G_k \alpha_k e^{-i\phi_k}\right)^n}{\sqrt{n!}} |n\rangle \tag{2.10}$$

can be used to represent laser pulses emitted from a QKD transmitter. In turn, a pair of these coherent pulse states can be used to model the time-bin superposition states generated in the BB84 protocol[2].

2.2.2 Asymmetric Mach-Zehnder Interferometer (AMZI)

The primary element of the measurement system is an AMZI, which overlaps and interferes the two laser pulses being measured. Firstly, the model of the AMZI will need to include two beam splitters, used to create the two paths of the interferometer. Beam splitters

[2]See appendix B.2.2 for details on the evolution of a coherent laser pulse through an AMZI.

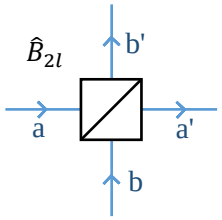


Figure 2.3: Simple schematic of a beam splitter (operation $\hat{B}_{2l}$) with input spatial modes a and b and output spatial modes a' and b'.

with two-spatial-mode inputs, a and b, will be considered, as shown in figure 2.3. The operation of this beam splitter on the coherent state $|\alpha\rangle_a |\beta\rangle_b$ is given by [46, 47],

$$\hat{B}_{2l} |\alpha\rangle_a |\beta\rangle_b = |\sqrt{T_l}\alpha - i\sqrt{R_l}e^{i\psi_{Bl}}\beta\rangle_{a'} |\sqrt{T_l}\beta - i\sqrt{R_l}e^{-i\psi_{Bl}}\alpha\rangle_{b'} \tag{2.11}$$

where a' and b' are the output spatial modes, T_l is the transmittance, R_l is the reflectance, ψ_{Bl} is the imparted phase shift and l is a distinguishing index to differentiate multiple beam splitters.

The AMZI contains two paths that the input light can propagate through, each imparting its own phase shift and attenuation in the light. The effect of attenuation on the coherent state can be modelled by employing the beam splitter operation and performing a partial trace on the output state. The derivation is shown in appendix B.2.1, resulting in the following operator equation,

$$\hat{A}_j |\alpha\rangle_j = |\sqrt{\eta_j}\alpha\rangle_j \tag{2.12}$$

where j is the spatial mode ($j = a, b, a', b'$) and η_j is the optical transmittance. The phase shift operator shown in equation 2.8 can be used to represent the phase shift imparted by the AMZI arms,

$$\hat{P}_j |\alpha\rangle_j = |e^{-i\psi_j}\alpha\rangle_j \tag{2.13}$$

where j is once again the spatial mode and ψ_j is the imparted phase shift. The beam splitter, attenuation and phase shift operations can be combined to construct a model of the measurement system AMZI, shown in figure 2.4. In this setup, laser pulses are emitted from the QKD transmitter and are initially sent to beam splitter $\hat{B}_{20}$, which transmits some of the light to the AMZI and reflects the rest towards a monitoring detector DM[3]. The light sent to the AMZI is split by beam splitter $\hat{B}_{21}$, creating the two interferometer paths a and b. Light travelling through arm a (b) undergoes a phase shift ψ_a (ψ_b) imparted by $\hat{P}_a$ ($\hat{P}_b$), and passes through attenuator $\hat{A}_a$ ($\hat{A}_b$), with a transmittance of η_a (η_b). Both arms are then recombined at beam splitter $\hat{B}_{22}$, which has two outputs leading to detectors D1 and D2.

Two coherent pulses labelled k and k+1 are input into the measurement system shown in figure 2.4, where these pulses are represented by $|G_k\alpha_k e^{-i\phi_k}\rangle$ and $|G_{k+1}\alpha_{k+1}e^{-i\phi_{k+1}}\rangle$ respectively. Applying the operations 2.11 - 2.13 for the system, equations for the output power at each detector can be derived. The temporal delay of the AMZI is set such that the part of pulse k travelling through path b and the part of pulse $k+1$ travelling through path a are overlapped and interfered at $\hat{B}_{22}$. Equations for the resulting detected optical powers are calculated, which are in turn used to calculate the power ratios; the optical

[3]This monitoring detector is not particularly intended for use with QKD pulses at the single-photon level, as it would result in unnecessary loss applied to the QKD signal. However, the monitoring detector is important when using bright light within an interferometer, the importance of which will be discussed in section 2.4.

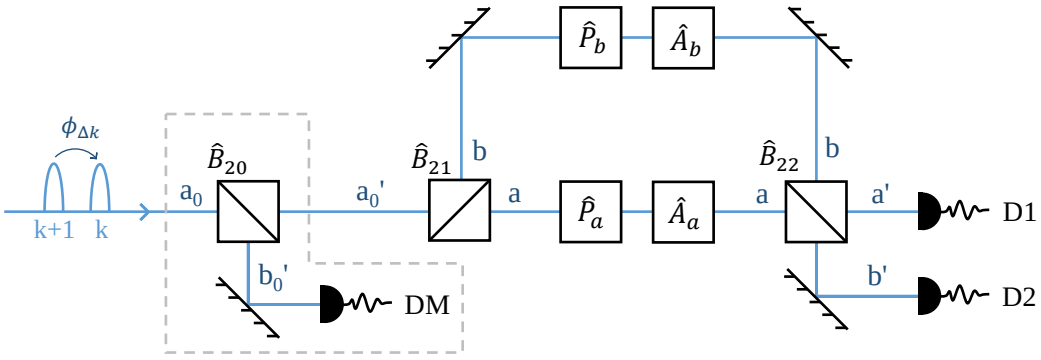


Figure 2.4: Diagram of the measurement system AMZI model, consisting of beam splitters ($\hat{B}_{20}$, $\hat{B}_{21}$, $\hat{B}_{22}$), detectors (DM, D1, D2), phase shifters ($\hat{P}_a$, $\hat{P}_b$) and attenuators ($\hat{A}_a$, $\hat{A}_b$). The temporal delay between the arms of the AMZI is set such that pulses k and $k+1$ are overlapped.

powers detected at D1 and D2 divided by that detected at DM. Calculation of the power ratios removes any fluctuations in the power of the signal input into the AMZI. This results in the following equations,

$$P_{R1} = \frac{P_1}{P_M} = \frac{1}{2}\left[S_1 - D_1 \cos\left(\phi_Q + \psi_{Int}\right)\right] \tag{2.14}$$

$$P_{R2} = \frac{P_2}{P_M} = \frac{1}{2}\left[S_2 + D_2 \cos\left(\phi_Q + \psi_{Int}\right)\right] \tag{2.15}$$

where,

$$P_M = \eta_M R_0 |\alpha_k|^2 \tag{2.16}$$

and R_0 is the reflectance of beam splitter $\hat{B}_{20}$. See appendix B.2 for details of the derivation, where it is assumed that $|\alpha_k|^2 = |\alpha_{k+1}|^2$. The sum terms ($S_1$, S_2) and difference terms (D_1, D_2) are calculated by performing a sweep of the interferometer phase ψ_{Int}, which produces an interference pattern of the power ratio. From this, the maximum and minimum power ratio of the pattern can be used to calculate the sum and difference terms as follows,

$$S_1 = P_{Rmax1} + P_{Rmin1} \tag{2.17}$$

$$D_1 = P_{Rmax1} - P_{Rmin1} \tag{2.18}$$

$$\tag{2.19}$$

where P_{Rmax1} (P_{Rmin1}) is the maximum (minimum) power ratio detected at D1. The same can be done for the power ratio detected at D2. The original phase difference between the pulses is given by,

$$\phi_Q = \phi_{k+1} - \phi_k \tag{2.20}$$

where ϕ_k and ϕ_{k+1} are the phases of pulses k and $k+1$ respectively. The phase shift imparted by the AMZI between the pulses is given by,

$$\psi_{Int} = \psi_b - \psi_a + \psi_{B1} - \psi_{B2} \tag{2.21}$$

where ψ_a (ψ_b) is the phase shift applied by $\hat{P}_a$ ($\hat{P}_b$) and ψ_{B1} (ψ_{B2}) is the phase shift incurred when passing through beam splitters $\hat{B}_{21}$ ($\hat{B}_{22}$). Equation 2.14 can be rearranged to give an equation for the original phase difference between the two pulses,

$$\phi_Q + \psi_{Int} = \cos^{-1}\left(\frac{1}{D_1}\left[S_1 - 2P_{R1}\right]\right) + \chi_1 \tag{2.22}$$

where χ_1, termed the falling or rising factor, is used to unwrap the phase from the $[0, \pi]$ range to the $[0, 2\pi)$ range. This is done by determining whether a phase measurement is made on a falling or rising edge of the interference pattern; see appendix B.2.5 for further details. The same can also be applied to equation 2.15. If the optical path difference (OPD) between the arms a and b of the AMZI are varied, the values of ψ_a and ψ_b and therefore ψ_{Int} will vary also, resulting in an interference pattern at the output of the AMZI. From this the values of S_1 and D_1 can be determined, meaning that all the terms in equation 2.22 can be measured during an experiment. This avoids the need for a full characterisation of the measurement system prior to an experiment, which in practice would be difficult to achieve.

Varying the OPD over a longer distance, such that the value of ψ_{Int} repeatedly cycles through the [0, 2π) range, will result in many interference fringes at the AMZI output, where each of these fringes will be indistinguishable from one another. The full phase imparted by an AMZI path $j = a, b$ can be denoted by θ_j where,

$$\psi_j = \theta_j \qquad (\text{mod } 2\pi). \tag{2.23}$$

Therefore ψ_j is the remainder phase imparted by path j. To calculate the value of ϕ_Q between pulses k and $k+1$ for a characterisation measurement, only the value of ψ_{Int} must be determined, not the full path phases of θ_j. However, it is important to note the distinction between these phases as it is critical when considering the methods for determining the value of ψ_{Int}, discussed further in section 2.2.4.

2.2.3 Single-photon Detectors (SPDs)

When measuring signals at the single-photon level, the detectors DM, D1 and D2 in figure 2.4 can be replaced with the single-photon detectors SPDM, SPD1 and SPD2 [4]. It is assumed that the single-photon detectors are non-photon number resolving, only the binary outputs of the SPD (click or no-click) can be registered. An SPD may register a click for a number of reasons,

- True count; when a photon from the signal intended to be measured reaches the SPD.
- Dark count; an erroneous click resulting from thermally-activated counts or background photons.
- After-pulsing; an erroneous count that occurs after a detection due to trapped charges from the previous detection event. This is typically observed in single-photon avalanche photodiodes where large populations of electron-hole pairs are created.

For the purposes of the characterisation measurement, the dead time of the SPD's used will be set to minimise the effects of afterpulsing, so that the number of after-pulse counts is negligible. The true count and dark count probabilities for SPDl are denoted by p_{TCl} and p_{DCl}, where l =M,1,2. The true count detection probability can be used to calculate the detected mean photon number per pulse [41],

$$\mu_l = -\frac{1}{\eta_l} \ln\left(1 - p_{TCl}\right) \tag{2.24}$$

where η_l is the detection efficiency of SPDl. As the mean photon number per pulse is proportional to the optical power of the signal, equations similar to 2.14 and 2.15 can be

[4] Ideally here the mean single-photon number per pulse is consistent across the pulse train, so that there is no need for detector SPDM

derived for the single photon case. However, unlike for optical power that can be measured directly, the probabilities p_{TCl} cannot be determined from the detection of a single pair of pulses alone. Instead many pairs of pulses must be measured and the resulting variation in clicks can be used to determine the detection probabilities. When measuring many QKD pulses to determine the true-click probability it is important to either,

- Set the QKD transmitter to produce only the set phase difference intended to be measured, or
- During the measurement, record what phase the QKD transmitter was intending to send for every detection event, so that post-measurement the recorded counts can be sorted into groups of detections, where the groups are sorted according to one phase setting of each signal state or decoy states if these are employed.

For any measurement, a significant number of counts for a chosen transmitter setting must be collected for a range of values of ψ_{Int} to build up an interference pattern. The number of counts required will depend on the SPD used, see section 3.3.4 for further details. The value of ϕ_Q can therefore be determined and compared with the intended phase setting of the transmitter. To accommodate the other factors that affect the function of SPD's such as dead time, the appropriate pulse rates, detection gates and recovery times will be chosen to avoid spurious and invalid counts [22].

2.2.4 Resolving the Interferometer Phase

To determine the set phase difference between two QKD pulses, ϕ_Q, the phase shift imparted by the interferometer ψ_{Int} must be determined, as seen in equation 2.22. There are two methods of resolving the interferometer phase; the first is to measure the value of ψ_{Int} directly and the second is to only monitor the change, $\Delta\psi_{Int}$.

Method 1: Measure ψ_{Int} Directly

The ideal option is to measure the value of ψ_{Int} directly, but achieving this is not straightforward as it requires high accuracy length measurements with resolution on the nanometre scale. The most convenient way to perform this measurement is to input laser light of a known phase relationship into the AMZI and to use the resulting interference output to determine the imparted phase shift of the interferometer. For example, if CW laser light is input the initial phase difference $\phi_Q = 0$, such that equation 2.22 reduces to,

$$\psi_{Int} = \cos^{-1}\left(\frac{1}{D_1}\left[S_1 - 2P_{R1}\right]\right) + \chi_1 \tag{2.25}$$

allowing ψ_{Int} to be calculated directly. However, this value is dependent on the wavelength of the input light and therefore the signal used must have the same wavelength as the QKD signal to obtain an accurate value of ψ_{Int} for the QKD light under test. Furthermore, due to the effect of external influences on the measurement system, the value of ψ_{Int} may vary over the duration of the characterisation measurement. Therefore, either the value of ψ_{Int} must be monitored over the course of the characterisation procedure or it must be stabilised to an appropriate level to avoid large errors in the resulting phase measurements. The nuances of this issue will be explored in further detail in section 2.4.

Method 2: Measure the Change, $\Delta\psi_{Int}$

An alternative option is to determine the change in the interferometer phase $\Delta\psi_{Int}$, where this can either be monitored using laser light, or can be set to $\Delta\psi_{Int} \approx 0$ by appropriately

stabilising the interferometer. This allows the change in the QKD signal phase $\Delta\phi_Q$ between different phase settings to be determined. For example, for a pair of pulses k and $k+1$ with phase difference ϕ_Q, and another pair of pulses k' and $k'+1$ with phase difference ϕ'_Q, the change in phase is given by,

$$\begin{aligned}\Delta\phi_Q &= \phi_Q - \phi'_Q \\ &= \cos^{-1}\left(\frac{1}{D_1}\left[S_1 - 2P_{R1}\right]\right) - \cos^{-1}\left(\frac{1}{D_1}\left[S_1 - 2P'_{R1}\right]\right) + \Delta\chi_1 - \Delta\psi_{Int}\end{aligned} \tag{2.26}$$

where $\Delta\chi_1 = \chi_1 - \chi'_1$ and $\Delta\psi_{Int} = \psi_{Int} - \psi'_{Int}$. The values of the two cosine terms and $\Delta\chi_1$ can be readily determined, such that the change in phase between different phase settings $\Delta\phi_Q$ can be calculated. This approach is less challenging experimentally than the previous method, however, as it only measures the change in phase setting $\Delta\phi_Q$, it may not be suitable for characterising all phase-based features of a QKD transmitter.

In both of the methods detailed, there is a need to stabilise and monitor the interferometer phase ψ_{Int} during the characterisation process, which is explored further in the following sections.

2.3 Interferometer Stability & Temperature

Changes in the OPD between the two arms of the interferometer varies the imparted interferometer phase shift ψ_{Int}. To avoid this, the optical path lengths (OPL) of the AMZI arms, a and b, must be stabilised, where each of the arms may be constructed out of various combinations of optical materials. The combined OPL of one of the interferometer arms can represented as,

$$OPL_j = \sum_m n_m L_{jm} \tag{2.27}$$

where $j = a, b$ represents the interferometer arm, m represents the optical material, n_m is the refractive index of material m and L_{jm} is the length of material m in arm j. Here it is assumed that the refractive index of material m is homogeneous in the direction of travel of the light. The OPD between the two arms a and b is therefore given by,

$$OPD = OPL_a - OPL_b = \sum_m n_m L_{abm} \tag{2.28}$$

where $L_{abm} = L_{am} - L_{bm}$. The OPL determines the full phase shift imparted by an arm of the interferometer onto the input light, where this full phase shift is represented by θ_j as defined in equation 2.23. The full phase imparted by each arm can therefore be defined as,

$$\theta_j = \frac{2\pi}{\lambda} OPL_j = \frac{2\pi}{\lambda} \sum_m n_m L_{jm} \tag{2.29}$$

where the full phase difference imparted by the interferometer is then given by,

$$\theta_{Int} = \theta_a - \theta_b = \frac{2\pi}{\lambda} \sum_m n_m L_{abm} \tag{2.30}$$

This is the unbounded interferometer phase, that is not restricted by the $[0, 2\pi)$ range. Therefore, the phase difference imparted by the AMZI can be written as,

$$\psi_{Int} = \theta_{Int} \pmod{2\pi} \tag{2.31}$$

where ψ_{Int} is restricted to the $[0, 2\pi)$ range. The value of ψ_{Int} is directly dependent on the refractive index and length of the optical materials, both of which are temperature dependent. To stabilise the interferometer and minimise variation in ψ_{Int}, the temperature of the interferometer must be controlled.

2.3.1 Change in Interferometer Phase with Temperature

Changes in the temperature of the interferometer and its surroundings can affect the OPD via two processes, thermal expansion and the thermo-optic effect. Thermal expansion results in the expansion or contraction of the material, changing the physical lengths of the interferometer arms. For each material m, the extent of this effect is parametrised by the thermal expansion coefficient α_m defined as,

$$\alpha_m = \frac{1}{L_m}\frac{dL_m}{dT} \tag{2.32}$$

where L_m is the initial material length and T is the temperature. The thermo-optic effect is the change in the refractive index of a material with temperature, which varies the optical path length experienced by light propagating through that material. The extent of this effect is determined by the thermo-optic coefficient defined as,

$$\beta_m = \frac{dn_m}{dT} \tag{2.33}$$

where n_m is the refractive index of material m. Assuming that the temperature change experienced by both arms of the interferometer is the same, the change in the value of θ_{Int} with temperature is given by,

$$\frac{d\theta_{Int}}{dT} = \frac{2\pi}{\lambda}\sum_m \left(n_m\alpha_m + \beta_m\right) L_{abm} \tag{2.34}$$

A similar derivation can be found in [48]. The temperature sensitivity increases linearly with the asymmetry of the AMZI, L_{abm}. To assess the stability of different optical materials for use in the AMZI, equation 2.34 is rearranged to give,

$$\frac{1}{L_{abm}}\frac{d\theta_{Int}}{dT} = \frac{2\pi}{\lambda}\left(n_m\alpha_m + \beta_m\right) \tag{2.35}$$

which it termed the phase-temperature sensitivity. The value of this is calculated and compared for different optical materials.

Air

For free-space beams travelling through air in an interferometer, the thermo-optic coefficient β_{air} must be determined, but the thermal expansion coefficient $\alpha_{air} = 0$, as the thermal expansion of air does not change the physical length of the interferometer arm. To determine the value of β_{air}, the refractive index of air can be calculated using the Edlén equation [49–52] over a temperature range, and the resulting variation can be substituted into equation 2.33. The value of n_{air} resulting from the Edlén equation is dependent upon the wavelength of the light, the air pressure, the relative humidity and the air temperature. Taking the wavelength of the light to be 1550 nm; typical for telecommunications, the standard air pressure of 101.325 kPa and the relative humidity to be 50 %, the resulting variation in n_{air} over temperature is shown in figure 2.5. The least-squares fit line in figure 2.5 has a gradient of $\beta_{air} = -9.47 \pm 0.04 \times 10^{-7}\ K^{-1}$, which when substituted into equation 2.34 results in a phase-temperature sensitivity of,

$$\frac{1}{L_{ab\,air}}\frac{d\theta_{Int}}{dT} = \frac{2\pi}{\lambda}\beta_{air} = -3.84 \pm 0.02\ \mathrm{radm^{-1}K^{-1}}. \tag{2.36}$$

A similar method for calculating the thermo-optic coefficient of air is performed in [53].

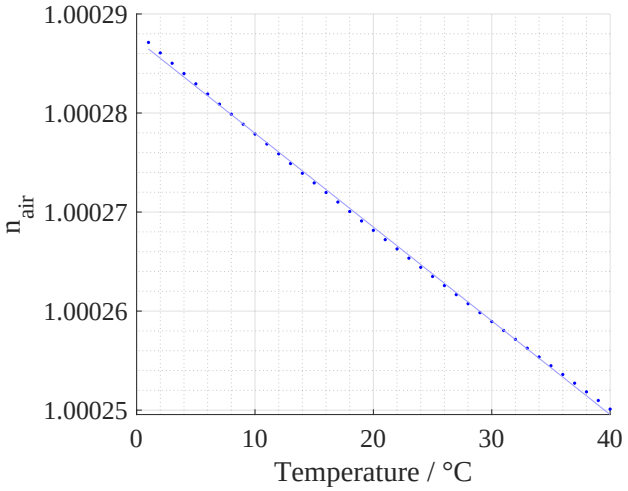


Figure 2.5: Refractive index of air as a function of temperature for 1550 nm light. The blue points are values of the refractive index given by the Edlén equation[49–52] assuming standard air pressure of 101.325 kPa and a relative humidity of 50 %. The light blue line is the least-squares fit of the refractive index, where the gradient of this line provides an approximate value for β_{air} over this temperature range.

Waveguide: Optical Fibre

The other primary material option for constructing the interferometer is optical fibre, which is used extensively in telecommunication networks and QKD system installations. Optical fibres are particularly useful in interferometry as they can be used to create long interferometer paths with a much smaller spatial footprint compared to free-space optical setups. Fibre systems also require far less optical alignment, particularly when connecting and disconnecting individual fibre-optic patch cords, which allows large changes to be made to the OPD of an AMZI by simply adding or removing patch cords. However, conservation of the mode of the laser light in optical fibre is typically less straightforward when compared to free-space beams and requires specialised optics, such as polarisation-maintaining (PM) fibre, critical for interferometry.

Estimates for the phase-temperature sensitivity of optical fibre can be predicted using equation 2.34 and values of the refractive index, thermal expansion coefficient and the thermo-optic coefficient. A guide value of phase-temperature sensitivity can be determined using published values of these variables. For example, for Corning 7980 fused silica the following values apply:

$n_{C7980} = 1.44502$	For light at 1500 nm at 21.85°C [54]
$\alpha_{C7980} = 0.52 \times 10^{-6}$ K^{-1}	Between $5 - 35$°C [55]
$\beta_{C7980} = 8.45 \times 10^{-6}$ K^{-1}	For light at 1500 nm at 21.85°C [54]

These yield a phase-temperature sensitivity of,

$$\frac{1}{L_{ab\,C7980}} \frac{d\theta_{Int}}{dT} = 38.54 \text{ radm}^{-1}\text{K}^{-1}. \tag{2.37}$$

approximately ten times greater than that for air.

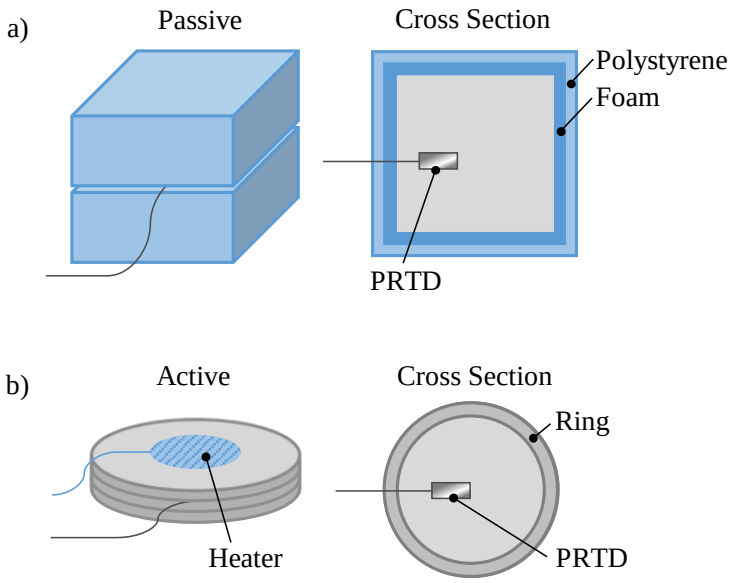


Figure 2.6: Schematics depicting the experimental setups for temperature control, including cross-section views. a) shows the passive setup consisting of a insulating box containing the platinum resistance temperature detector (PRTD). b) shows the active setup consisting of a set of metal disks and resistive heaters linked to a PID temperature controller.

2.3.2 Achievable Temperature Stability

Given the predicted phase-temperature sensitivities, the temperature stability can be assessed to determine the maximum phase stability of an AMZI in a laboratory-based setting. Two approaches to stabilising the temperature of an interferometer are via passive or active methods, both of which are assessed. The chosen passive control consists of a large $30 \times 30 \times 30$ cm metal box base and lid, each surrounded by a 2 cm layer foam and a 3 cm layer of polystyrene, as depicted in figure 2.6a). A platinum resistance temperature detector (PRTD) is placed within the box, which is then sealed with the lid, such that the lid and base layers overlap, blocking air currents and reducing temperature fluctuations.

In comparison the active temperature control method consists of a set of heaters attached to aluminium plates, which are controlled using a Wavelength Electronics PTC5K-CH temperature controller [56]. The plates consist of two solid disks and a ring, all with a diameter of 30 cm and a thickness of 8 mm. The plates are bolted together in the order of disk-ring-disk, producing a cavity inside, in which a PRTD is placed[5] as depicted in figure 2.6b). On activating the temperature controller, the temperature of the plates is increased to ~ 30 °C, around 8 °C higher than the laboratory environment temperature. The temperature controller includes a PID loop that continually monitors the temperature and adjusts the power supplied to the heaters to maintain the temperature of the plates.

The temperature inside the two setups was recorded over a 65-hour time period, starting after a stabilisation period of 77.5 hours for the passive setup and a 11.5 hour stabilisation period for the active setup. This stabilisation time started at the point the box was closed for the passive case, and once the temperature controller and heaters were switched on in the active case. The recorded temperatures are split into 15-minute time intervals and the maximum temperature change in each interval is recorded in the histograms in

[5]Advice sought from colleagues at the National Physical Laboratory contributed towards these measurements.

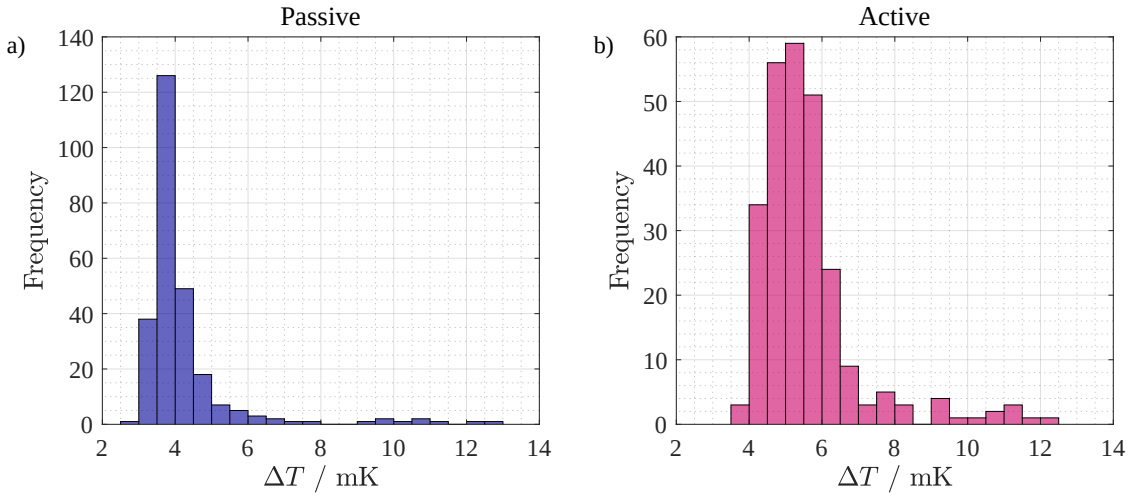


Figure 2.7: Histograms of the maximum temperature change per 15-minute interval over a 65 hour measurement period. a) shows the temperature change for the passive temperature control setup after a stabilisation period of 77.5 hours. b) shows the temperature change for the active temperature control setup after a stabilisation period of 11.5 hours. Note that the y-axis of the active case has a lower range.

figure 2.7.

Both temperature control methods show similar temperature stability. The passive setup provides slightly better stability with a mean maximum temperature change of 4.24 mK per 15-minute interval, compared to a mean of 5.62 mK for the active case. However, the passive system required a much longer stabilisation period compared to the active case. Taking the phase-temperature sensitivity values for air and optical fibre previously calculated in equations 2.36 and 2.37 respectively, the resulting change in phase $\Delta\psi_{Int}$ can be calculated for the average change in temperature over the 15-minute interval in the passive and active cases. For a typical QKD system, the pulse repetition rate is ~ 1 GHz, equivalent to a temporal separation of 1 ns. To overlap adjacent pulses in this pulse train, an AMZI asymmetry of $L_{ab\,air} = 30$ cm or $L_{ab\,fib} = 20$ cm is required. The anticipated phase change over a 15-minute interval at these asymmetries is shown in table 2.1. In

Temperature Control	**Material**	
	Air	Fibre
Passive	-4.88 mrad	45.6 mrad
Active	-6.47 mrad	60.5 mrad

Table 2.1: Predicted values of $\Delta\psi_{Int}$ over a 15-minute interval for a free space AMZI ($L_{ab\,air} = 30$ cm) and a fibre AMZI ($L_{ab\,fib} = 20$ cm) under passive or active temperature control. The values are calculated using the phase-temperature sensitivity values for air (equation 2.36) and fibre (equation 2.37) and the average temperature changes for the passive and active temperature control setups from the data shown in figure 2.7.

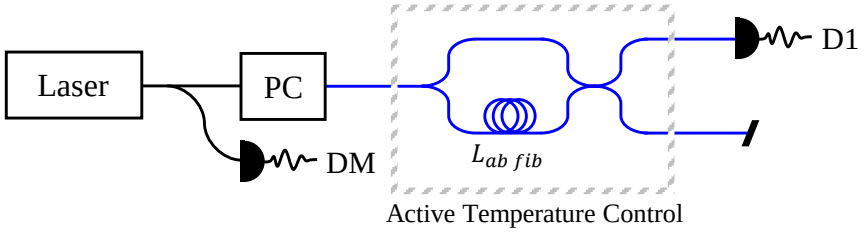


Figure 2.8: Diagram of the experimental setup used to determine the phase-temperature sensitivity of optical fibre. The setup consists of a laser light source, polarisation control (PC) and detectors (DM, D1). Black lines indicate single-mode optical fibre and blue lines indicate single-mode polarisation-maintaining fibre. The AMZI is constructed out of two fibre-optic 50:50 couplers and a fibre loop of length $L_{ab\ fib} = 20$ cm, which is contained within an actively-temperature controlled area (grey dashed box).

addition to these estimates, the phase stability of an AMZI can also be determined by directly measuring the variation using a monitoring laser light.

2.3.3 Direct Measurement of Phase Stability

To directly assess the phase stability of an AMZI, frequency-stable[6] CW laser light is propagated through the system and the resulting interference fringes are assessed to determine the drift in phase. An optical fibre AMZI system was constructed as shown in figure 2.8, consisting of a CW laser at 1550 nm, a polarisation controller and photodiodes. The AMZI has an OPD of $L_{ab\ fib} = 20$ cm and is actively temperature controlled, in a similar form to that described in section 2.3.2. The optical power detected is used to calculate the phase shift imparted by the interferometer via equation 2.22, where $\phi_Q = 0$ and the phases recorded all sit on one edge of an interference fringe such that $\chi_1 = 0$. The maximum change in the interferometer phase per 15-minute interval are histogrammed in figure 2.9, where it is assumed that the wavelength of the laser light is constant over the course of each 15-minute interval. The average change in phase imparted by the AMZI is $\Delta\phi_{Int} = 30.67$ mrad, which is not dissimilar to the predicted value for active temperature control of fibre shown in table 2.1.

For a characterisation measurement that lasts 15 minutes, if these values of $\Delta\psi_{Int}$ are not monitored, they directly translate into errors on the final phase measurement value. These errors are relatively small when compared to the minimum separation between phase settings in QKD protocols, for example the encoding states of phase-encoded BB84 [17] have a separation of $\pi/2 = 1.57$ rad. In addition, for the discrete phase randomisation described in [36], the minimum separation between phase settings is $2\pi/10 = 0.628$ rad. However, for AMZI's with much longer path lengths or for measurement setups not based in ideal temperature control conditions, these phase changes and therefore the phase measurement error may increase significantly beyond the precision required for the phase characterisation measurement. Furthermore, the stabilisation time for both the passive and active setup are impractical, particularly for characterisation measurements that must be performed on location, outside of the lab. Therefore the stability of the surrounding environment of the AMZI cannot be relied upon to adequately stabilise the interferometer phase ψ_{Int} and instead this property will need to be monitored during the course of the characterisation measurement using some form of reference laser light signal.

[6]Section 2.4.5 explores the phase error as a function of frequency/wavelength change of the laser signal.

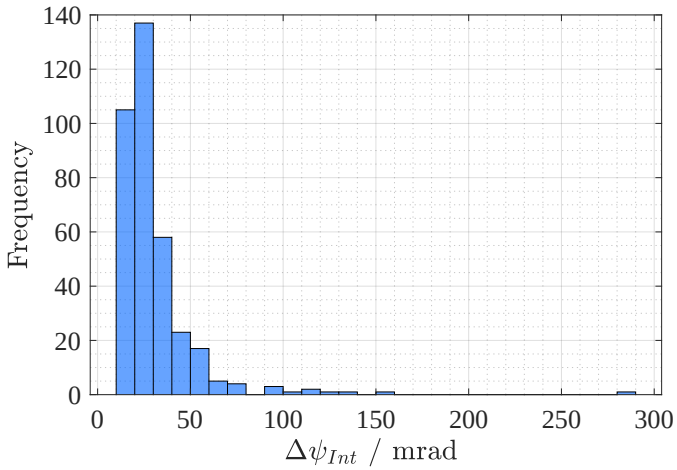


Figure 2.9: The maximum change in phase imparted by the AMZI, $\Delta\psi_{Int}$, per 15-minute interval.

2.4 Reference Signal for Interferometer Stabilisation

2.4.1 Reference Laser Light

To monitor the interferometer phase ψ_{Int} of the AMZI over the duration of a characterisation measurement a reference laser signal can be used. This reference light must be relatively bright compared to the single-photon level QKD signal, so that the current value of ψ_{Int} can be determined from a single recorded data point of the reference signal. The optical power of the reference signal can be detected using power meters, in the same setup as shown in figure 2.4. The output power of the reference signal can then be substituted into equation 2.25 to determine the interferometer phase as perceived by the reference signal, which is given by,

$$\psi_{IntR\,[0,\pi]} = \cos^{-1}\left(\frac{1}{D_{1R}}\left[S_{1R} - 2\frac{P_{1R}}{P_{MR}}\right]\right) \tag{2.38}$$

$$\psi_{IntR\,[0,2\pi)} = \psi_{IntR\,[0,\pi]} + \chi_{1R} \tag{2.39}$$

where $\psi_{IntR\,[0,\pi]}$ is the phase bounded within the the $[0,\pi]$ range and $\psi_{IntR\,[0,2\pi)}$ is the phase bounded within the $[0,2\pi)$ range. The other terms are as defined previously, where R subscripts has been added to indicate that these terms correspond to the reference signal. The interferometer phase as determined by the reference signal, ψ_{IntR}, can then be used to determine the interferometer phase shift experienced by the QKD signal, ψ_{IntQ}, which is explored in more detail in section 2.4.3.

The implementation of both the QKD signal and the reference light into the same optical system must be carefully considered, primarily so that the reference signal can be separated from the QKD signal. This is particularly important when considering the SPD's, as any stray bright light from the reference signal will increase the number of dark counts and may even damage the detectors. To avoid any mixing of the two signals, the reference wavelength can be chosen to be different to the QKD wavelength, but within the same band so that both signals are supported by the same optical components. Wavelength division multiplexers can then be used to separate the two signals prior to detection, removing the reference signal from the SPD input.

2.4.2 Monitoring the Interferometer Phase

The previous sections have concerned the measurement of the interferometer phase ψ_{Int} within the $[0, 2\pi)$ range. However, if the interferometer phase is adjusted and monitored carefully, such that the fringe edge type is continuously recorded and care is taken when traversing over the peaks and troughs of the interference pattern, it is possible to unwrap the change $\Delta\psi_{Int}$ to give the change in the overall interferometer phase $\Delta\theta_{Int}$. Monitoring the value of $\Delta\theta_{Int}$ can then be applied to the two methods described in section 2.2.4 to resolve the interferometer phase; or, more specifically, the interferometer phase experienced by the QKD signal ψ_{IntQ}.

Method 1: Measure ψ_{IntQ} Directly

When using a reference signal to monitor the change in the interferometer phase $\Delta\theta_{IntR}$, this can be converted into that experienced by the QKD signal $\Delta\theta_{IntQ}$. To then determine the value of ψ_{IntQ} directly an initial calibration step must be performed, which requires, ideally bright, laser light at the QKD wavelength with known phase properties, for example coherent CW light. During the calibration, this signal is passed through the AMZI along with the reference signal and the interferometer phase of these two signals is calculated. A single data point taken simultaneously for each signal can then be used as the starting phase, a phase value that every future phase measurement for both signals is referenced to. The starting phases are denoted by ψ_{IntQ0} for the QKD wavelength and ψ_{IntR0} for the reference signal wavelength. Throughout the measurement procedure, the change in the interferometer phase, $\Delta\theta_{IntQ}$ and $\Delta\theta_{IntR}$, can be added to the starting phases to determine the current value of the interferometer phase as follows,

$$\begin{aligned} \psi_{IntQ} &= \psi_{IntQ0} + \Delta\theta_{IntQ} \qquad (\text{mod } 2\pi) \\ \psi_{IntR} &= \psi_{IntR0} + \Delta\theta_{IntR} \qquad (\text{mod } 2\pi) \end{aligned}$$

where the application of (mod 2π) restricts the ranges of $\Delta\theta_{IntQ}$ and $\Delta\theta_{IntR}$ to $[0, 2\pi)$ to match the ranges of ψ_{IntQ} and ψ_{IntR}. Therefore this initial calibration step will allow the value of ψ_{IntQ} to be calculated directly, which in turn allows the QKD phase setting ϕ_Q to be determined.

Method 2: Measure the Change, $\Delta\psi_{IntQ}$

As with the previous method, the change in the interferometer phase for the reference signal $\Delta\theta_{IntR}$ can be used to calculate that for the QKD signal $\Delta\theta_{IntQ}$. Therefore, to determine the value of $\Delta\psi_{IntQ}$ only the following operation is needed,

$$\Delta\psi_{IntQ} = \Delta\theta_{IntQ} \qquad (\text{mod } 2\pi)$$

where the application of (mod 2π) restricts the range of $\Delta\theta_{IntQ}$ to $[0, 2\pi)$ to match the range of $\Delta\psi_{IntQ}$. Although this method does not require an extra calibration step, it only allows the difference between the QKD phase settings to be determined $\Delta\phi_Q$.

2.4.3 Phase Conversion between Reference and QKD Signals

To measure the phase of the QKD signal in both methods detailed previously, the change in the interferometer phase $\Delta\theta_{IntR}$ must be monitored by the reference laser light. However, as the reference signal and the QKD signal have different wavelengths, the phase shift

imparted by the interferometer will not be equivalent for the two signals. The phase shift imparted by the interferometer is written as,

$$\theta_{Intj} = \frac{2\pi}{\lambda_j} OPD_j \tag{2.40}$$

where $j = R, Q$ to differentiate the reference and QKD signal respectively. The refractive index n_{mj} is also given a subscript as it is dependent on the wavelength of the light. A change in the calculated interferometer phase $\Delta\theta_{Intj}$ can occur for the following reasons:

- A purposeful change in the physical asymmetry length of the interferometer, L_{abm}
- An unintended change in the surrounding temperature of the AMZI resulting in a change in the OPD
- An unintended change in the wavelength of the laser light

Therefore, at any point during the measurement procedure, a change in the interferometer phase can be written as a combination of these processes,

$$\Delta\theta_{Intj} = \Delta\theta_{Lj} + \Delta\theta_{Tempj} + \Delta\theta_{\lambda j} \tag{2.41}$$

where,

$$\Delta\theta_{Lj} = \frac{2\pi}{\lambda_j} \sum_m n_{mj} \Delta L_{abm} \tag{2.42}$$

$$\Delta\theta_{Tempj} = \frac{d\theta_{Intj}}{dT} \Delta T \tag{2.43}$$

$$\Delta\theta_{\lambda j} = \frac{2\pi}{\lambda_j} OPD_{\lambda j} - \frac{2\pi}{\lambda'_j} OPD'_{\lambda j}. \tag{2.44}$$

$\Delta\theta_{Lj}$ is the phase change due to an intended change in the path asymmetry. $\Delta\theta_{Tempj}$ is an unintended change in the phase due to the interferometer temperature varying by ΔT. $\Delta\theta_{\lambda j}$ is an unintended change in the phase due to a change in the signal wavelength from λ_j to λ'_j, where the OPD changes from $OPD_{\lambda j}$ to $OPD'_{\lambda j}$ as the refractive index is wavelength dependent. During the course of the measurement, purposeful changes to the AMZI path lengths will not be implemented using optical fibre and therefore equation 2.41 can be written as,

$$\Delta\theta_{Intj} = \frac{2\pi}{\lambda_j} n_{air\,j} \Delta L_{ab\,air} + \Delta\theta_{Tempj} + \Delta\theta_{\lambda j}. \tag{2.45}$$

Therefore the phase shift experienced by the QKD signal $\Delta\theta_{IntQ}$ can be calculated from that for the reference signal $\Delta\theta_{IntR}$ as follows,

$$\Delta\theta_{IntQ} = \frac{\lambda_R}{\lambda_Q} \frac{n_{airQ}}{n_{airR}} \Delta\theta_{IntR} + \varepsilon_{Temp} + \varepsilon_{\lambda} \tag{2.46}$$

where,

$$\varepsilon_{Temp} = \Delta\theta_{TempQ} - \frac{\lambda_R}{\lambda_Q} \frac{n_{airQ}}{n_{airR}} \Delta\theta_{TempR} \tag{2.47}$$

$$\varepsilon_{\lambda} = \Delta\theta_{\lambda Q} - \frac{\lambda_R}{\lambda_Q} \frac{n_{airQ}}{n_{airR}} \Delta\theta_{\lambda R} \tag{2.48}$$

are error terms due to unintended changes in temperature and wavelength that cannot be suitably measured within the characterisation system. The Edlén equation can be

used to calculate the value for n_{airQ}/n_{airR} for the QKD and reference wavelengths. The conversion equation for $\Delta\theta_{IntR}$ to $\Delta\theta_{IntQ}$ is therefore taken to be,

$$\Delta\theta_{IntQ} \approx \frac{\lambda_R}{\lambda_Q}\frac{n_{airQ}}{n_{airR}}\Delta\theta_{IntR}. \tag{2.49}$$

To determine the measurement error resulting from terms ε_{Temp} and ε_λ, their values must be estimated for typical conditions of the measurement system.

2.4.4 Estimating the Temperature Error Term

For the purposes of this assessment it is assumed that $n_{airQ}/n_{airR} \approx 1$, such that equation 2.47 can be written as,

$$\varepsilon_{Temp} = \left(\frac{d\theta_{IntQ}}{dT} - \frac{\lambda_R}{\lambda_Q}\frac{d\theta_{IntR}}{dT}\right)\Delta T \tag{2.50}$$

where,

$$\frac{d\theta_{Intj}}{dT} = \frac{2\pi}{\lambda_j}\sum_m \left(n_{mj}\alpha_m + \beta_{mj}\right) L_{abm} \tag{2.51}$$

which is the same as equation 2.34 with the subscripts $j = Q, R$ added to the appropriate terms. This form of the equation is useful when considering beams propagating in free-space, however equation 2.47 can also be written as,

$$\varepsilon_{Temp} = \frac{2\pi}{\lambda_Q}\left(\Delta OPD_{TempQ} - \Delta OPD_{TempR}\right) \tag{2.52}$$

which is useful when considering beams propagating in fibre. The overall temperature error term will have contributions from both air and optical fibre such that,

$$\varepsilon_{Temp} = \varepsilon_{Temp\,air} + \varepsilon_{Temp\,fib} \tag{2.53}$$

and each of the equations above can be used estimate the value of these contributions.

Air: Edlén Equation

The Edlén equation [49–52] can be used to assess the value of ε_{Temp} for a beam propagating through free-space. The thermal expansion coefficient for air is once again $\alpha_{air} = 0$ and equation 2.50 can be simplified to give,

$$\begin{aligned}\varepsilon_{Temp\,air} &= \frac{2\pi}{\lambda_Q}\left(\beta_{airQ} - \beta_{airR}\right) L_{ab\,air}\Delta T \\ &= \frac{2\pi}{\lambda_Q}\left(\Delta n_{airQ} - \Delta n_{airR}\right) L_{ab\,air}.\end{aligned} \tag{2.54}$$

The change in refractive index for the QKD and reference wavelength for various temperature changes can be calculated using the Edlén equation, providing an estimate for $\varepsilon_{Temp\,air}$. Values for $\varepsilon_{Temp\,air}$ are shown in figure 2.10 for varying asymmetry length $L_{ab\,air}$ and over a temperature range of 22 ± 1 °C. For typical OPL values and anticipated temperature variations, this error term will not greatly effect the final phase measurement error.

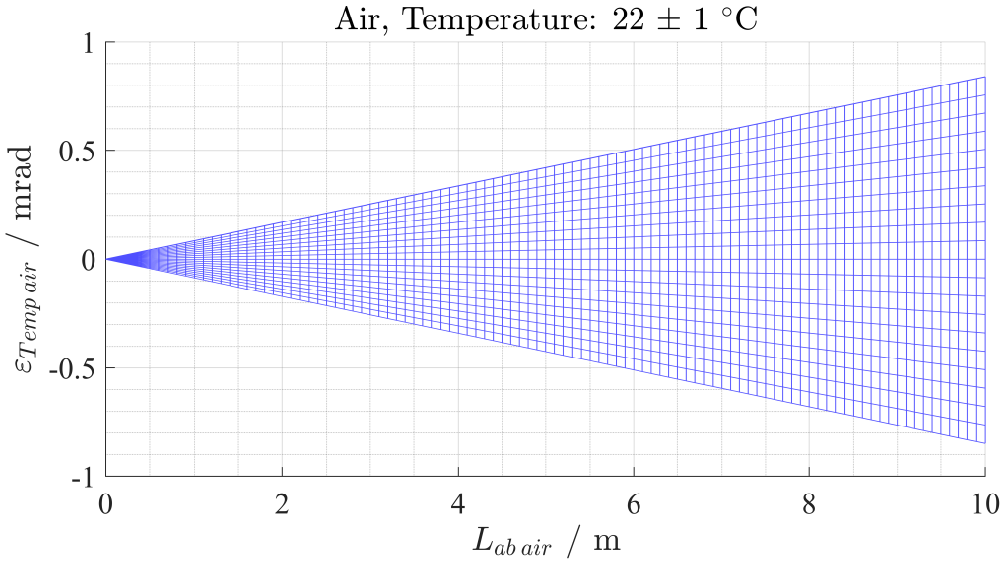


Figure 2.10: The phase-temperature error term for air is shown for varying asymmetry lengths ($L_{ab\,air}$) and over a temperature range of 22 ± 1 °C. The uppermost line traces the value of $\varepsilon_{Temp\,air}$ for 23 °C and the lowermost line traces the value of $\varepsilon_{Temp\,air}$ for 21 °C. The refractive index for air is calculated using the Edlén equation for a relative humidity of 50% and at the standard atmospheric pressure, 101.325 kPa. The QKD and reference signal wavelengths are taken to be 1550 nm and 1542 nm respectively.

Waveguide (Optical Fibre): Dispersion

To determine the contribution from optical fibre, $\varepsilon_{Temp\,fib}$, equation 2.52 can be used in combination with equations for dispersion in optical fibre. Dispersion is the difference in time taken for two photons separated by 1 nm in wavelength, to traverse a distance of 1 km. Dispersion is measured in units of ps/(nm·km) and is given by [58, 59],

$$D = \frac{S_0}{4}\left(\lambda - \frac{\lambda_0^4}{\lambda^3}\right) \tag{2.55}$$

where λ_0 is the wavelength at $D = 0$ and S_0 is the gradient of the dispersion curve at $\lambda = \lambda_0$. Data for the dispersion of Thorlabs PM1550-XP optical fibre, provided by Thorlabs [57], is shown in figure 2.11a) along with the least squares fit of equation 2.55. The resulting parameter values of the least squares fit are $S_0 = 0.0924$ ps/(km·nm^2) and $\lambda_0 = 1305.4$ nm. The difference between the two OPD's experienced by the QKD signal and the reference signal can be expressed in terms of the dispersion,

$$OPD_{fibQ} - OPD_{fibR} = L_{ab\,fib} c D \Delta\lambda \tag{2.56}$$

where c is the speed of light in a vacuum and $\Delta\lambda = \lambda_Q - \lambda_R$. The derivation is shown in appendix B.4.1. For variations in temperature, the path asymmetry length, $L_{ab\,fib}$, and the value of the fibre dispersion will change. The temperature dependence of optical fibre dispersion is given by [58, 59],

$$\frac{dD}{dT} = \frac{1}{4}\left(\lambda - \frac{\lambda_0^4}{\lambda^3}\right)\frac{dS_0}{dT} - \frac{S_0\lambda_0^3}{\lambda^3}\frac{d\lambda_0}{dT} \tag{2.57}$$

where S_0 and λ_0 both have temperature dependence. Using mean values for $dS_0/dT = -2.46 \times 10^{-6}$ ps/(nm^2·km·°C) and $d\lambda_0/dT = 0.026$ nm/°C from [58], which have been

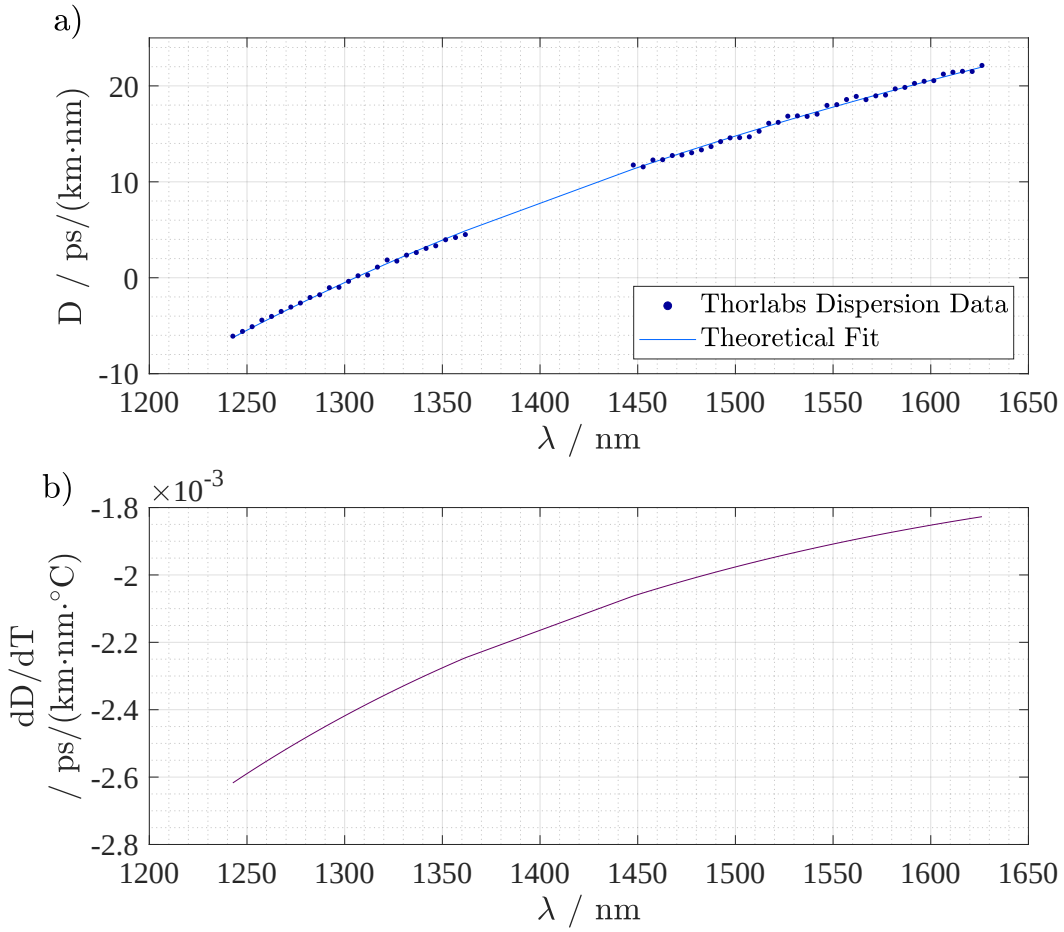


Figure 2.11: a) Thorlabs dispersion data [57] for PM1550-XP optical fibre and the least squares fit of equation 2.55, resulting in the following parameter values, $S_0 = 0.0924$ ps/(km·nm^2) and $\lambda_0 = 1305.4$ nm. b) Temperature dependence of the dispersion for the Thorlabs data, calculated using equation 2.57. The values of $dS_0/dT = -2.46 \times 10^{-6}$ ps/(nm^2·km·°C) and $d\lambda_0/dT = 0.026$ nm/°C from [58] are used.

calculated from experimental tests on a selection of optical fibres, the value of dD/dT is plotted in figure 2.11b) for the Thorlabs PM1550-XP dispersion data [57]. For a temperature change of ΔT, the difference in the change of the OPD for the QKD signal and reference signal is given by,

$$\Delta OPD_{fibQ} - \Delta OPD_{fibR} \approx \frac{dD}{dT} L_{ab\,fib} c \Delta T \Delta\lambda. \tag{2.58}$$

The derivation is shown in appendix B.4.1, where the approximation is due to the discounting of negligible terms. By combining this with equation 2.52, the temperature error term for optical fibre can be written as,

$$\varepsilon_{Temp\,fib} \approx \frac{2\pi}{\lambda_Q} \frac{\partial D}{\partial T} L_{ab\,fib} c \Delta T \Delta\lambda. \tag{2.59}$$

Values for $\varepsilon_{Temp\,fib}$ are shown in figure 2.12 for varying path asymmetry $L_{ab\,air}$ and over a temperature range of 22 ± 1 °C. For smaller lengths of fibre and appropriate temperature controls, as discussed in previous sections, the value of $\varepsilon_{Temp\,fib}$ should not greatly effect

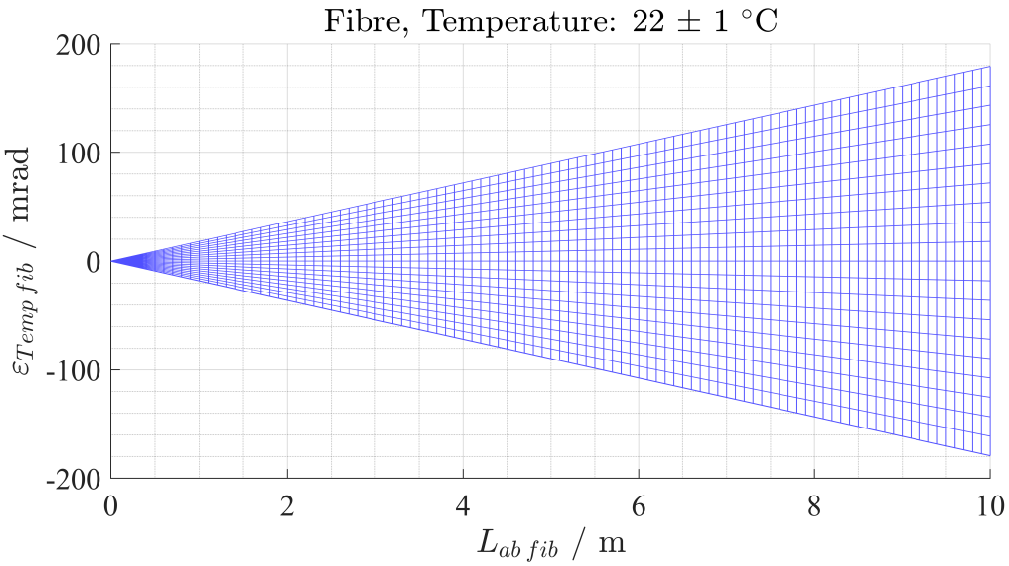


Figure 2.12: The phase-temperature error term for fibre is shown for varying asymmetry length ($L_{ab\,fib}$) and over a temperature range of 22 ± 1 °C. The uppermost line traces the value of $\varepsilon_{Temp\,fib}$ for 23 °C and the lowermost line traces the value of $\varepsilon_{Temp\,fib}$ for 21 °C. The error term is calculated using equation 2.59 and employs estimates for the values of $S_0 = 0.0924$ ps/(km·nm^2) and $\lambda_0 = 1305.4$ nm determined from fibre dispersion data from [57], and $dS_0/dT = -2.46 \times 10^{-6}$ ps/(nm^2·km·°C) and $d\lambda_0/dT = 0.026$ nm/°C from [58]. The QKD and reference signal wavelengths are taken to be 1550 nm and 1542 nm respectively.

the resulting phase measurement error. However, care should be taken when considering longer lengths of optical fibre, as achieving a smaller phase measurement uncertainty may require improved temperature controls.

2.4.5 Estimating the Wavelength Error Term

For the purposes of this error assessment it is assumed that $n_{airQ}/n_{airR} \approx 1$. It is also assumed that the wavelength of the QKD signal is consistent and does not change over the duration of the phase measurement, such that $\Delta\theta_{\lambda Q} = 0$. Equation 2.48 can therefore be written as,

$$\varepsilon_\lambda = -\frac{\lambda_R}{\lambda_Q}\Delta\theta_{\lambda R}. \tag{2.60}$$

The change in the phase $\Delta\theta_{\lambda R}$ can be written as follows,

$$\Delta\theta_{\lambda R} = \frac{2\pi}{\lambda_R - \Delta\lambda_R}\left(\Delta OPD_{\lambda R} - \frac{\Delta\lambda_R}{\lambda_R} OPD_{\lambda R}\right) \tag{2.61}$$

where $\Delta OPD_{\lambda R} = OPD_{\lambda R} - OPD'_{\lambda R}$ is the change in the OPD experienced by the reference signal due to the change in the reference signal wavelength $\Delta\lambda_R = \lambda_R - \lambda'_R$. The derivation for this is shown in appendix B.3. To estimate the error term, the value of ΔOPD_R must be evaluated for both air and optical fibre where,

$$\varepsilon_\lambda = \varepsilon_{\lambda\,air} + \varepsilon_{\lambda\,fib}. \tag{2.62}$$

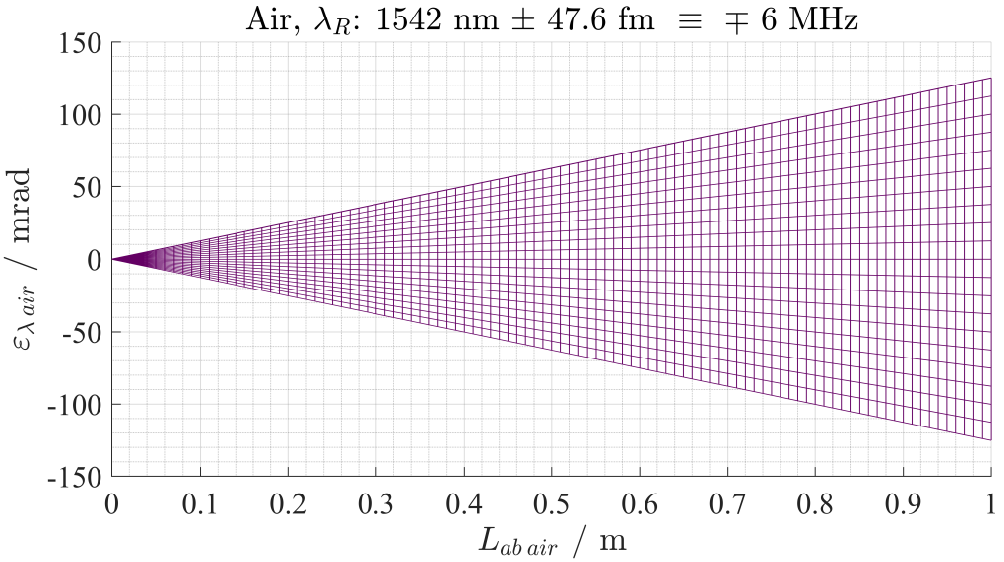


Figure 2.13: The phase-wavelength error term for air is shown for varying asymmetry length ($L_{ab\,air}$) and for a wavelength shift in the reference signal of up to ±47.6 fm, equivalent to ∓6 MHz. The uppermost line traces the value of $\varepsilon_{\lambda\,air}$ for $\lambda_R - 47.6$ fm and the lowermost line traces the value for $\lambda_R + 47.6$ fm. The refractive index for air is calculated using the Edlén equation for a relative humidity of 50% and at the standard atmospheric pressure 101.325 kPa. The QKD and reference signal wavelengths are taken to be 1550 nm and 1542 nm respectively. Note that the values of $L_{ab\,air}$ only extend up to 1 m.

Air: Edlén Equation

For air, the error term can be calculated using the Edlén equation [49–52] as before. By using equations 2.60 and 2.61, and taking,

$$\Delta OPD_{\lambda R\,air} = \Delta n_{airR} L_{ab\,air} \tag{2.63}$$

the error term is given by,

$$\varepsilon_{\lambda\,air} = -\frac{\lambda_R}{\lambda_Q}\frac{2\pi}{\lambda_R - \Delta\lambda_R}\left(\Delta n_{airR} - \frac{\Delta\lambda_R}{\lambda_R} n_{airR}\right) L_{ab\,air} \tag{2.64}$$

where $\Delta n_{air\,R}$ is the change in the refractive index experienced by the reference light due to a change in wavelength. Values for $\varepsilon_{\lambda\,air}$ are shown in figure 2.13 for varying $L_{ab\,air}$ and frequency shift in the reference signal of ±6 MHz. The value of 6 MHz is chosen as this is the stability of the reference laser, see section 3.4 in chapter 3. For this wavelength/frequency stability, the contribution of this phase error is not negligible and must be incorporated into the phase measurement uncertainty.

Waveguide (Optical Fibre): Dispersion

The error term for optical fibre can once again be calculated using the equations for dispersion. From equation 2.56 the change in the OPD for a shift in the reference signal wavelength of $\Delta\lambda_R$ can be written as,

$$\Delta OPD_{\lambda R} = L_{ab\,fib} c D \Delta\lambda_R \tag{2.65}$$

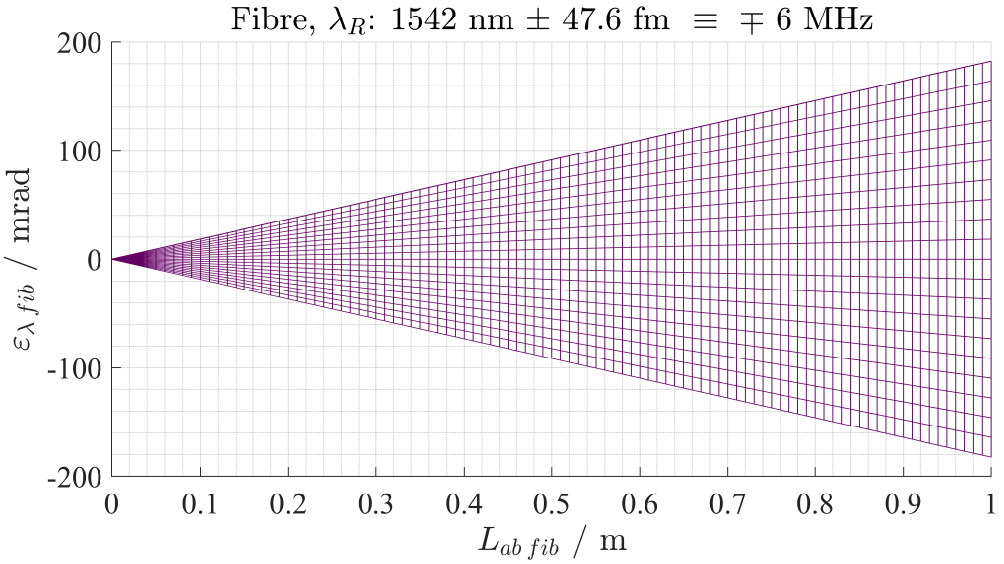


Figure 2.14: The phase-wavelength error term for fibre is shown for varying asymmetry length ($L_{ab\, fib}$) and for a wavelength shift in the reference signal of up to ±47.6 fm, equivalent to ∓6 MHz. The uppermost line traces the value of $\varepsilon_{\lambda\, fib}$ for $\lambda_R - 47.6$ fm and the lowermost line traces the value for $\lambda_R + 47.6$ fm. The error term is calculated using values for optical fibre dispersion from [57]. The QKD and reference signal wavelengths are taken to be 1550 nm and 1542 nm respectively. Note that the values of $L_{ab\, air}$ only extend up to 1 m.

and the resulting error term is given by,

$$\varepsilon_{\lambda\, fib} = -\frac{\lambda_R}{\lambda_Q}\frac{2\pi}{\lambda_R - \Delta\lambda_R}\left(cD - \frac{n_{fibR}}{\lambda_R}\right) L_{ab\, fib}\Delta\lambda_R \tag{2.66}$$

the derivation of which is shown in appendix B.4.2. The resulting values of $\varepsilon_{\lambda\, fib}$ for varying $L_{ab\, fib}$ and a frequency shift in the reference signal of ±6 MHz are shown in figure 2.14. The error term for optical fibre is larger than that for air, and once again must be included in the calculation of the phase measurement uncertainty when required.

2.5 Stabilisation at an Arbitrary Phase

Although there are advantages to using a reference laser light as a feedback signal to stabilise an AMZI, an inherent issue with this technique is that the sensitivity of the feedback will vary over the values of ψ_{IntR}. As the optical power output is dependent on the cosine of the interferometer phase, the feedback will be most sensitive on the edge of an interference fringe. Whereas, at the peak and trough, changes in the interferometer phase will result in much smaller shifts in the output power, and therefore will be far less sensitive. This results in an AMZI that can only be effectively stabilised, to the required standard, for specific values of ψ_{IntR}. To highlight this effect, equation 2.38 is used to produce the following equation for the change in the interferometer phase as perceived by the reference signal,

$$\Delta\psi_{IntR\,[0,\pi]} = \psi_{IntR\,[0,\pi]} - \cos^{-1}\left(\frac{2}{D_{1R}}\frac{\Delta P_{1R}}{P_{MR}} + \cos\left(\psi_{IntR\,[0,\pi]}\right)\right) \tag{2.67}$$

where $\Delta\psi_{IntR\,[0,\pi]} = \psi_{IntR\,[0,\pi]} - \psi'_{IntR\,[0,\pi]}$ and $\Delta P_{1R} = P_{1R} - P'_{1R}$ is the change in the detected optical power at the output of the AMZI. It is assumed that the monitoring power

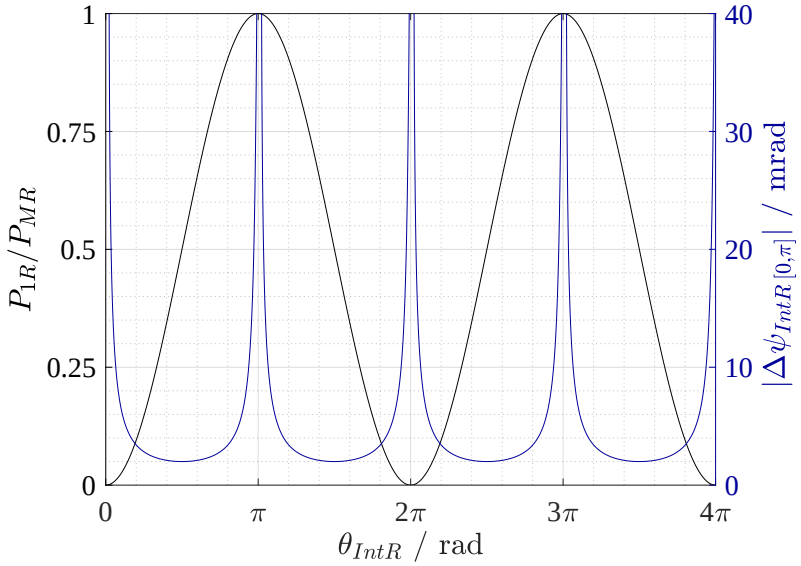


Figure 2.15: The interference pattern of a single mode of the reference light (black) and the resulting minimal resolvable change in the interferometer phase $\Delta\psi_{IntR}$ (blue). It is assumed that the interferometer is perfectly balanced, $D_{1R} = 1$, and the detector sensitivity is such that $\Delta P_{1R}/P_{MR} = 10^{-3}$.

P_{MR}, and the sum and difference terms S_{1R} and D_{1R} are consistent over the phase change. The derivation of this expression is shown in appendix B.5. To estimate the minimum resolvable phase change, the value of $\Delta P_{1R}/P_{MR}$ can be set to equal the detector sensitivity for the reference signal, which is typically $\Delta P_{1R}/P_{MR} = 10^{-3}$. For this sensitivity, the minimum resolvable phase change $\Delta\psi_{IntR}$ is plotted for varying θ_{IntR} in figure 2.15. For this it is also assumed that the interferometer is perfectly balanced, such that $D_{1R} = 1$. The minimum resolvable change in the interferometer phase increases greatly near the peaks and troughs, to an extent that would greatly effect the measurement uncertainty of the final stated phase value of the QKD signal if the AMZI was stabilised at these values of ψ_{IntR}.

Although it may be possible to perform a characterisation measurement of a QKD transmitter whilst avoiding particular AMZI phase settings of ψ_{IntR}, it is not an ideal design for the system and may effect the versatility of the measurement. Therefore it is important to resolve this sensitivity issue if possible.

2.5.1 Phase-Shifted Orthogonal Polarisation States

One way to improve the reference signal feedback sensitivity over all values of ψ_{IntR} is to use two separate modes of reference light. This method, explored in [60], can be implemented in the measurement system by generating two orthogonal polarisation modes of the reference light and sending them through the interferometer. Applying a phase delay between the two polarisation states of $\pi/2$ results in two interference patterns that are offset from one another, as shown in figure 2.16. Using both of these interference signals to stabilise the interferometer, the minimum resolvable phase difference is far better across arbitrary values of ψ_{IntR}, also shown in figure 2.16.

Sending and preserving two polarisation states of light simultaneously in free-space beams is relatively easy to accomplish, however achieving the same in optical fibre is a more complex task. PM fibre should be able to maintain the polarisation states that are aligned to either the slow or fast axis of the fibre, however this is not necessarily the case

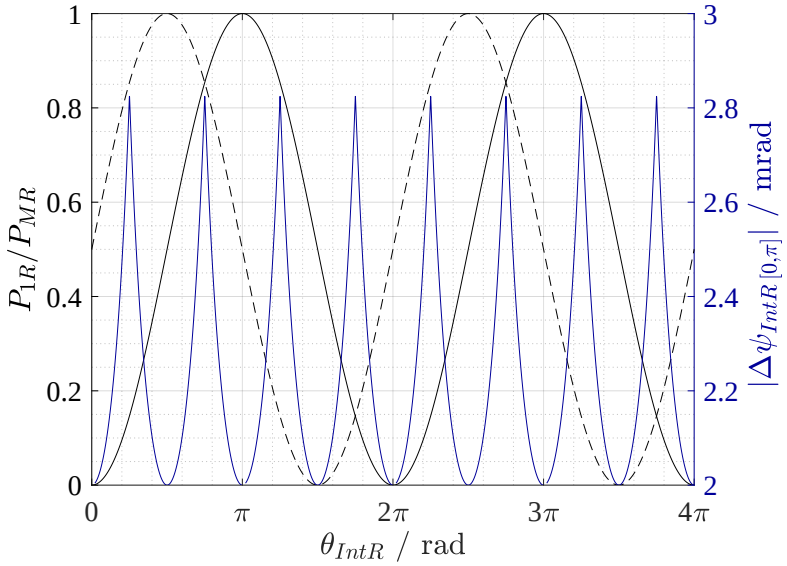


Figure 2.16: The minimum resolvable change in the interferometer phase $\Delta\psi_{IntR}$ (blue plot) for two reference interference patterns (black solid and dashed lines) resulting from two orthogonal polarisation states. One polarisation state experiences θ_{IntR} and the other experiences $\theta_{IntR} + \pi/2$ when propagating through the AMZI, resulting in the interference patterns being offset from one another. It is assumed that the interferometer is perfectly balanced, $D_1 = 1$, and the detector sensitivity is $\Delta P_1/P_M = 10^{-3}$. Note that the range of the right y-axis for $\Delta\psi_{IntR}$ is much smaller than that for figure 2.15.

when both polarisation states are sent simultaneously. To assess this, the experimental setup shown in figure 2.17 was constructed, consisting of a laser, polarisation controls, 5 m of PM fibre contained within the active temperature control setup described in section 2.3.2, a polarisation splitter and two detectors. The polarisation controls were set to produce either slow, fast or 45° diagonal polarisation, where the diagonal polarisation is equivalent to sending the slow and fast polarisation states at the same time. The slow and fast polarisation states are generated using a fibre-coupled linear polariser and optical fibres where the fibre connector key is set to align either the slow-to-slow axes or the slow-to-fast axes. The 45° diagonal polarisation state is generated using a linear polariser and a half waveplate rotated by 22.5° from the optical axis. The light is then propagated through the PM fibre while the temperature controlled plates are allowed to passively cool from a starting temperature of 27 °C down to 23 °C. The light is separated into its slow and fast aligned components by a fibre-coupled polarisation splitter, where the power at both outputs of the splitter is detected and recorded. The variation in the proportion of slow and fast aligned light output is calculated using the following equations,

$$R_S = \frac{\eta_1 \Delta P_S}{\eta_1 P_S + \eta_2 P_F}$$

$$R_F = \frac{\eta_2 \Delta P_F}{\eta_1 P_S + \eta_2 P_F}$$

where η_1 (η_2) is the detection efficiency of detector D1 (D2), P_S and P_F are the optical powers detected for the slow and fast output respectively and ΔP_S (ΔP_F) is the change in P_S (P_F) . The values for R_S and R_F are plotted in figure 2.18 for the data sets taken using the experimental setup described above.

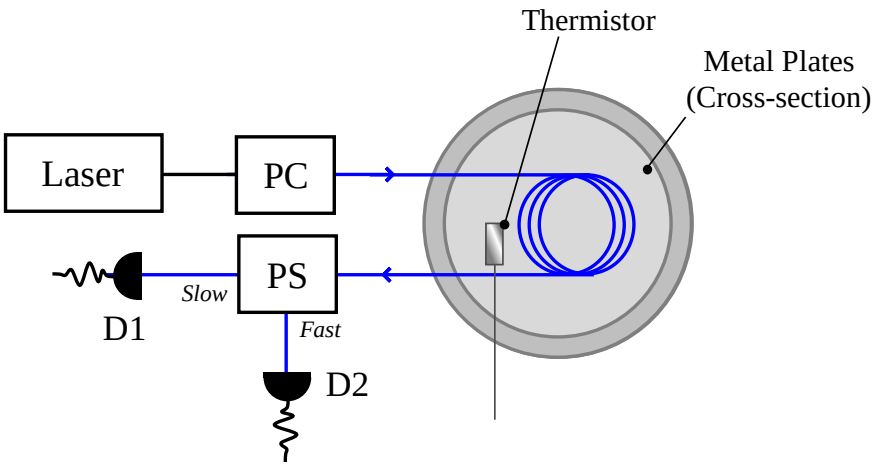


Figure 2.17: Setup used to test the stability of polarisation states in temperature varying PM fibre. The setup consists of a laser, polarisation controls (PC), a 5 m loop of PM fibre (blue lines), a polarisation splitter (PS) and detectors (D1, D2). The optical fibre is housed within the active temperature setup described in section 2.3.2.

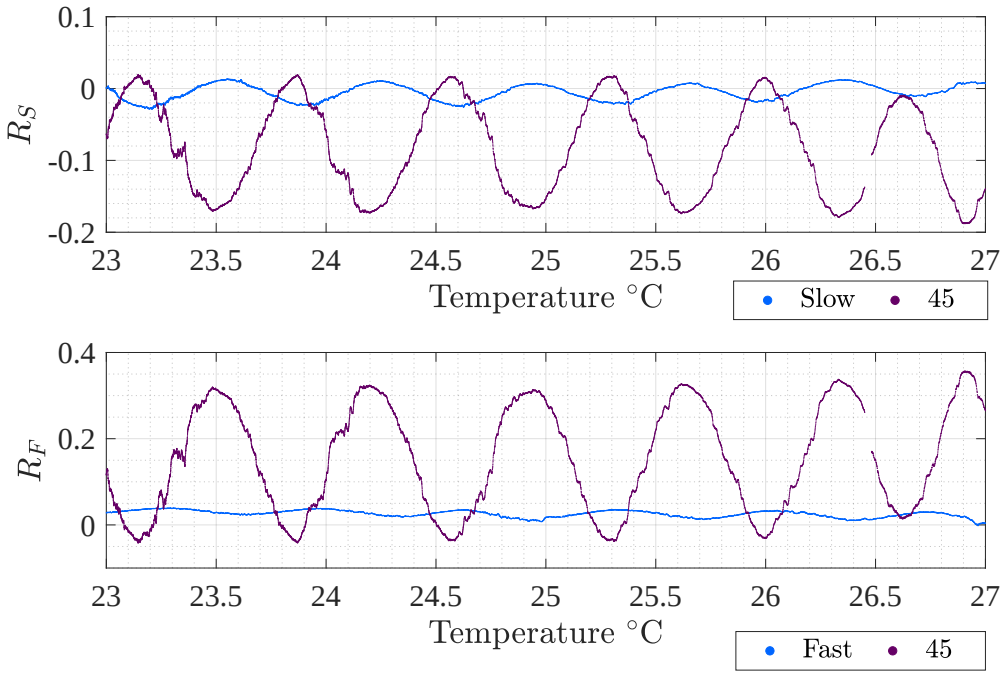


Figure 2.18: Plots of the variation in the ratio of slow and fast polarisation states against the total input power. Light aligned to the slow (fast) axis is used to calculate the value of R_S (R_F), and light in the 45° diagonal state is used to calculate both the value of R_S and R_F.

The value of R_S is calculated for the slow and 45° diagonal polarisation settings and the value of R_F is calculated for the fast and the same 45° diagonal polarisation settings. It is clear that in both cases the variation in transmittance of the slow and fast polarisations is far greater when propagating light in the 45° diagonal state, compared to the case when the slow and fast states are sent alone. Therefore, the crosstalk between the slow and fast polarisations is greater when sending the states simultaneously. As such, if two modes of polarised light are used to stabilise a measurement system containing optical fibre, the polarisation states should be sent through the system separately.

2.6 System Design Requirements

The models and measurement methods explored in this chapter can be used to distil a set of requirements for the design of the measurement system for phase characterisation. The following summarises the main points of interest.

2.6.1 Stabilisation with Feedback from a Reference signal

For improved system control and higher levels of measurement stability, a reference signal should be used to stabilise the AMZI. The reference signal will act as feedback for a PID loop, or similar feedback system, that controls a path shifting element within one of the interferometer arms. This reference light must have a known phase relationship, a known wavelength and it must have an acceptable level of frequency stability over the course of the measurement procedure. The reference signal must also be well isolated from the QKD signal, which may be achieved by reducing the optical power of the reference light and implementing isolators or wavelength division multiplexers into the system.

For an optimal phase stabilisation routine at arbitrary OPD settings of the AMZI, the reference signal should be prepared in two orthogonal polarisation states and the AMZI should include an element equivalent to a waveplate that produces a phase shift between the two polarisation states of $\pi/2$. This will result in the two interference patterns for each of the polarisations being offset, such that feedback for the stabilisation loop can be taken from the edge of the interference fringe for arbitrary values of ψ_{Int}. If optical fibre is to be used within the measurement system, the polarisation states should be sent into the system individually in an alternating pattern. Additionally, if optical fibre is implemented within or directly before the inputs to the AMZI, the fibre must be polarisation maintaining and the orthogonal polarisation states must be aligned to the slow and fast axes of the PM fibre.

When using a reference signal to monitor the variation in the phase shift imparted by the AMZI, $\Delta\theta_{IntR}$, where this is used to calculate the same phase shift imparted to the QKD signal, $\Delta\theta_{IntQ}$, care must be taken to assess the contribution of the error terms ε_{Temp} and ε_{λ}. These error terms must be incorporated into the calculations for the measurement uncertainty of the final stated phase values.

2.6.2 Calibration Routines

For calculation of the QKD and reference signal phases it will be necessary to perform calibration routines prior to and during the measurement procedure. This will include a sweep of the interferometer phase from 0 to 2π, which will produce an interference pattern allowing the minimum and maximum values of the output signals to be recorded, which can then be used in equation 2.22. In addition, to allow the calculated phase to be unwrapped from the range $[0, \pi]$ to the range $[0, 2\pi)$, the type of fringe edge (rising or falling), i.e. the sign of the gradient, must be determined and recorded throughout the

measurement procedure. The edge type can be determined by applying very small changes to the OPD and monitoring the resulting variation in output optical power.

2.6.3 Temperature Control

Even when employing a reference signal to stabilise the interferometer, temperature control will still be required to improve the stability of the AMZI. In particular, passive temperature controls that remove air currents will be critical in reducing the requirements imposed upon the reference signal feedback system.

Chapter 3

Design, Construction and Testing of the Measurement System

3.1 Measurement System Overview

The previous chapter highlighted the critical elements required to construct a measurement system to perform phase characterisation of quantum key distribution (QKD) hardware. On the basis of this, the measurement system can be separated into three primary elements,

- An Asymmetric Mach-Zehnder interferometer (AMZI)
- Reference signal preparation and detection
- QKD signal detection/probe signal generation, for the characterisation of transmitters/receivers

The ways in which these elements are combined for the characterisation of transmitter and receiver devices is shown in figure 3.1. For the characterisation of a QKD transmitter module, the measurement system must be used in conjunction with single-photon detectors, to measure the interference of the QKD signal. For the characterisation of a QKD receiver module, the measurement system must be combined with a laser source to produce a probe signal that can be used to measure the phase properties of the receiver. The AMZI element has two inputs, InR and InQ, and two outputs, $OutR$ and $OutQ$, where R and Q indicate whether that output is used for the reference or the QKD/probe signal. The reference signal and the QKD/probe signal are purposefully sent into the AMZI such that they propagate in opposite directions[1] to one another, allowing easier separation of the two signals prior to detection. This was inspired by [61].

As each of these primary elements of the measurement system are separate from one another, the measurement system can be used to test a range of QKD transmitters or receivers by simply connecting the AMZI input InQ or output $OutQ$ to the corresponding device. This chapter explores the primary elements of the measurement system in more detail, focussing on the construction, development of test procedures, data analysis and preliminary testing of the system. The measurement procedures and tests explored focus on cases where the measurement system would be used to characterise a QKD signal sent from a transmitter device, however much of this is still applicable when characterising receivers.

[1] Prior to the measurements conducted in this work, the reference and QKD signals are sent into the system separately and the optical power is measured at the inputs and outputs of the system, ensuring that the signals are not present at the wrong detectors or the laser inputs.

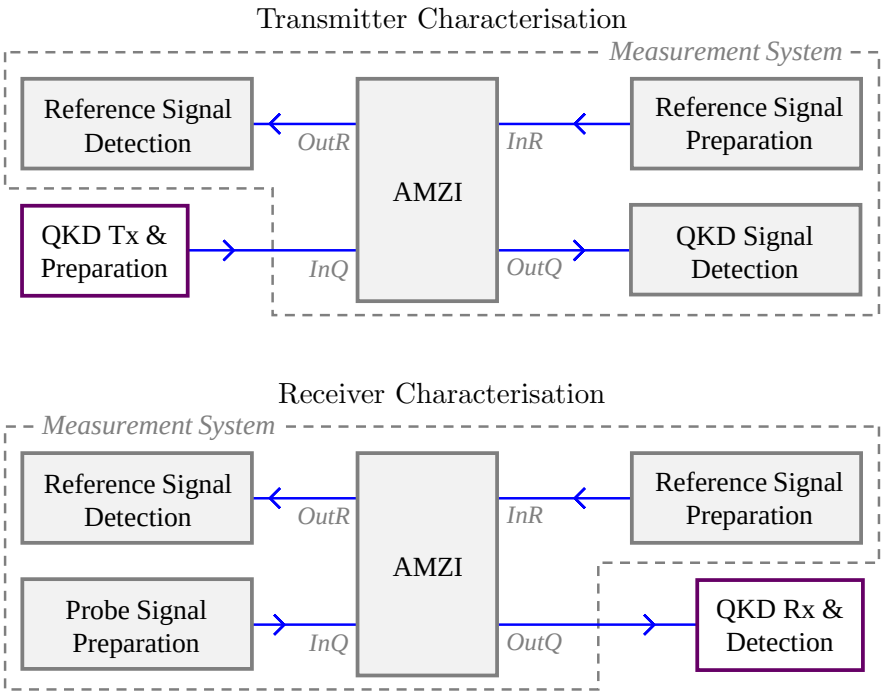


Figure 3.1: The combination of the primary elements of the measurement system for the characterisation of a QKD transmitter (QKD Tx) signal and for the characterisation of a QKD receiver (QKD Rx). The measurement system comprises the reference signal preparation and detection, AMZI, and either QKD signal detection or probe signal preparation. The AMZI inputs and outputs are labelled *InR*, *InQ* and *OutR*, *OutQ* respectively, where the *R* and *Q* refer to the reference and QKD/probe signals.

3.1.1 AMZI

The AMZI provides the path asymmetry which overlaps and interferes the incoming QKD pulses so that their phase can be determined. The optical path difference (OPD) of the AMZI must be stable enough to allow the reference laser feedback system to monitor changes in the interferometer phase $\Delta\theta_{IntR}$ (see equation 2.41). The OPD must also be adjustable, where there are three required levels of adjustment,

- Pulse selection, the largest part of the path asymmetry that determines the temporal separation between the two pulses to be interfered
- Pulse overlap tuning, a shorter adjustment range that is used to ensure the chosen pulses are accurately overlapped
- Phase sweep and adjustment, the shortest range of tuning with the highest precision that can incrementally step through the interference fringe of the output light

The ranges and incremental steps for each of these levels of path adjustment are detailed in table 3.1. These requirements can be used to inform the selection of the materials used to construct the arms of the AMZI, dependent on their suitability to provide the required level of path control. For pulse selection, using optical fibre to achieve the longer OPD lengths is convenient compared to free-space beams, as achieving the adjustable range in free-space would require precise alignment of optics with a large optical table footprint and would take an extended period of time for alignment when changing between delay lengths.

Path Control Level	Range	Incremental Precision
Pulse Selection	> 15 cm	5 cm
Pulse Overlap Tuning	$0 \rightarrow 5$ cm	0.3 mm
Phase Sweep and Adjustment	$0 \rightarrow 2$ μm	< 100 nm

Table 3.1: Estimates for the required ranges and incremental precision of the step sizes for each of the levels of OPD adjustment. The lengths stated here correspond to free-space interferometer arms, such that the refractive index $n \approx 1$.

For pulse selection and phase tuning, given the shorter adjustable ranges, it is possible to use free-space beams, which provide more OPD stability when compared to optical fibre. Furthermore, phase adjustments made in free-space allow for easier conversion between the change in the interferometer phase experienced by the reference signal ($\Delta\theta_{IntR}$) and that experienced by the QKD signal ($\Delta\theta_{IntQ}$), as explored in section 2.4.3.

On the basis of these requirements of the OPD, a custom interferometer element was procured to form part of the measurement system. Discussions were held with the manufacturer to specify the requirements of the device and establish the custom components and design needed for this interferometer. This interferometer element, named the wavelength-tunable micro interferometer (WT-MINT), was constructed by Kylia, the former optical division of Photonetics [62]. The WT-MINT (300 ps version [63]) consists of a compact (16.3×9.2 cm) housed free-space interferometer containing various optical components. One of the optical elements is placed on an actuator controlled stage and can be used to perform the pulse overlap tuning. Another optical element is placed on a piezo actuator and can be used to perform the phase sweep and adjustment. Alone, the WT-MINT is an AMZI with both interferometer arms contained within the housing box and with an adjustable OPD range from $0 \rightarrow 9$ cm. However, by flipping a switch, one of the interferometer arms can be tapped out of the device allowing the OPD to be extended above 9 cm. The interferometer arm that is always contained within the WT-MINT is referred to as the internal arm and the arm that can either be kept within the WT-MINT or tapped outside of the device is termed the external arm. The internal arm of the WT-MINT contains an attenuator, so that the loss in the two paths of the interferometer can be balanced to achieve higher visibility in the interference pattern. When the WT-MINT is set to the tap-enabled state, such that the external arm exits the WT-MINT housing, the length of the external arm can be extended by using either free-space optics or a combination of free-space and fibre-optic components. Figure 3.2 shows a schematic of the AMZI element and a photograph is shown in figure 3.3. In the free-space or fibre extension to the external arm, a Soleil-Babinet compensator (SBC) may be incorporated, which is an adjustable waveplate constructed from a birefringent plate and two wedges. The optical axis of the wedges is perpendicular to that of the plate and one of the wedges can be translated, as shown in figure 3.4, varying the amount of material that the incoming beam propagates through. If a beam is input into the SBC with a polarisation aligned to either the optical axis of the wedges or the plate, then the beam polarisation will not change, but the light will experience a delay. By adjusting the position of the moveable wedge, the delay experienced by light aligned to the wedge's optical axis can be varied, compared to the delay experienced by light aligned to the plate's optical axis. For the measurement system, the SBC allows a variable delay to be created between the slow and fast polarisations of the reference signal, where these polarisations are aligned to the optical axes of the SBC.

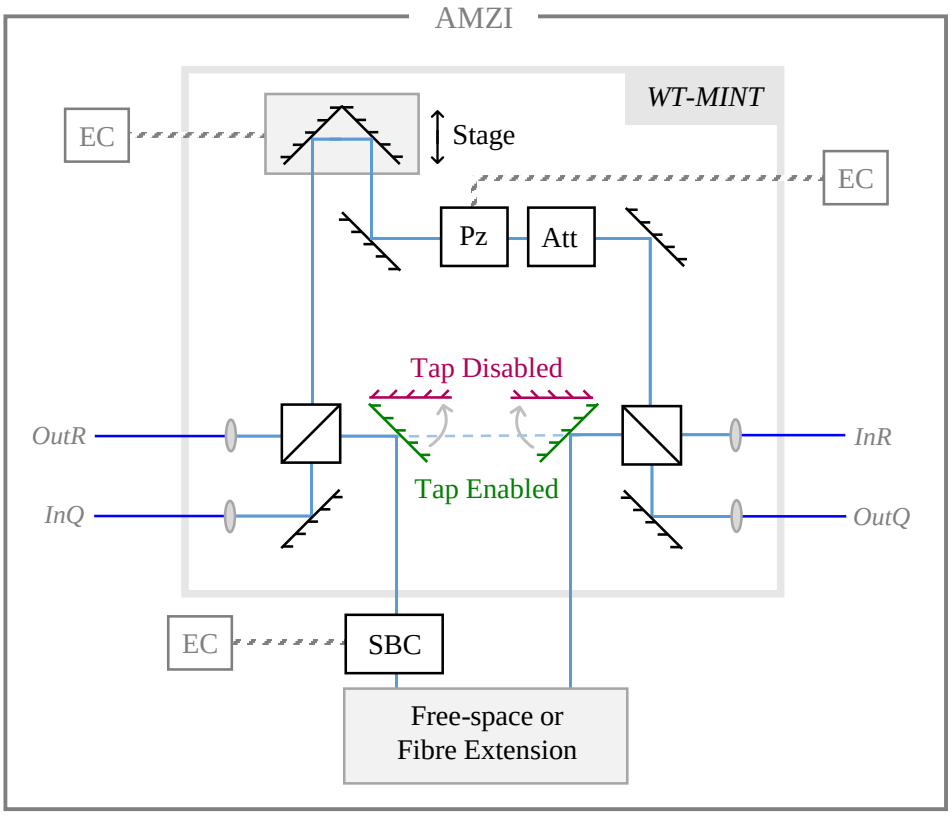


Figure 3.2: A schematic of the AMZI element of the measurement system, consisting of the wavelength-tunable micro interferometer (WT-MINT), Soleil-Babinet compensator (SBC) and the external arm extension constructed from free-space or fibre optics. The interferometer contains an actuator controlled optical stage (Stage), a piezo phase delay element (Pz), an optical attenuator (Att) and 50:50 beamsplitters. The two retractable mirrors can be set to either the "Tap Enabled" state (green) or the"Tap Disabled" state (red). In the tap-enabled state, the external interferometer arm exits the WT-MINT housing and propagates through the free-space or fibre extension. In the tap disabled state the external arm remains within the WT-MINT housing and propagates along the dashed light blue line. Elements of the system that are electronically controlled (EC) are indicated. Note that the layout of this schematic indicates the functionality of the WT-MINT, but is not necessarily a true representation of the internal setup.

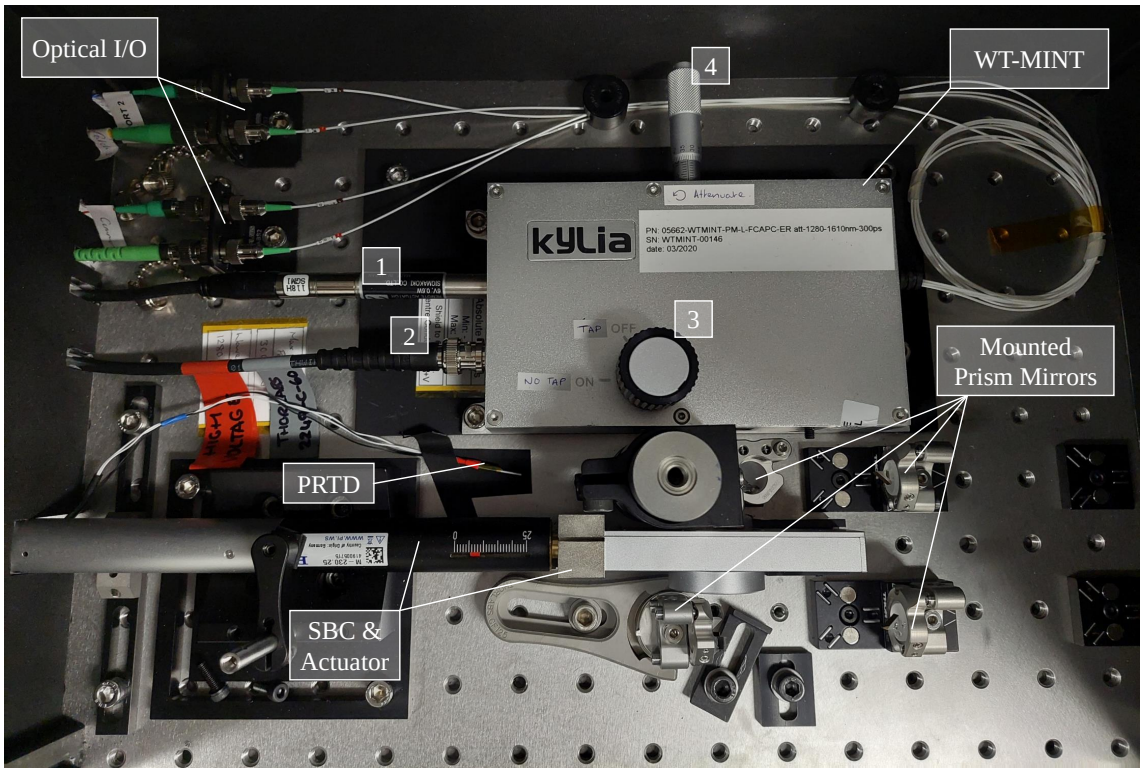


Figure 3.3: A photograph of the AMZI element of the measurement system, shown in figure 3.2. The components shown are labelled where I/O stands for inputs and outputs and PRTD stands for platinum resistance temperature detector. Elements of the WT-MINT are numbered, where 1 is the stage actuator, 2 is the piezo voltage supply, 3 is the tap-enabled or disabled switch and 4 is the manual control for the attenuator. The AMZI is setup with a free-space extension external to the WT-MINT, constructed using the mounted prism mirrors. A schematic of this free-space extension is shown in figure 3.5.

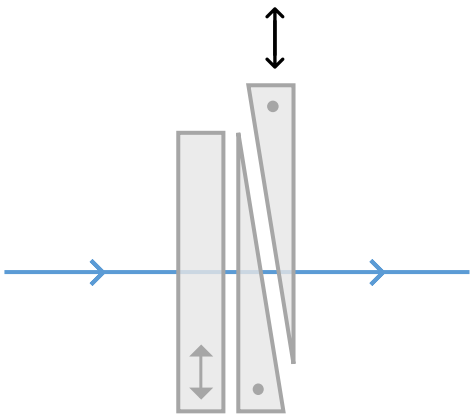


Figure 3.4: Basic construction of an SBC consisting of a plate and two wedges made of a birefringent material. The optical axes of the components are indicated by the grey arrow and dots, where the optical axis of the wedges is perpendicular to that of the plate. The beam propagates through the SBC along the light blue line and the offset wedge is moveable in the direction indicated by the black arrow.

As this delay is variable, a phase difference of $\pi/2$ between the slow and fast polarisations can always be achieved, as the SBC can compensate for phase shifts accumulated between the two polarisation states within the rest of the interferometer. This is particularly important when using polarisation-maintaining (PM) optical fibre within the interferometer arms, as the slow and fast aligned polarisations will experience different phase shifts in the fibre due to the different refractive indices associated with the slow and fast fibre axes. The SBC used in the measurement system is the RKQ 10 by B.Halle Nachfl. GmbH [64], consisting of a quartz plate and wedges, where the wedge translation is controlled by a Physik Instrumente M-230.25 actuator [65] and C-863.11 controller [66].

The setups of both the free-space extension and the fibre extension to the tap-enabled external arm are shown in figure 3.5. The free-space extension consists of six right-angle prism mirrors, where four of these mirrors are fixed and the remaining two are mounted on magnetic bases that can be moved to vary the length of the beam path. The output windows on the body of the WT-MINT housing are separated by 13 mm in the horizontal direction and separated by 2.9 mm in the vertical direction. Two of the fixed prism mirrors are placed end to end in the vertical plane to create a retroreflecting element that vertically displaces the beam to accommodate the vertical separation of the WT-MINT outputs.

The free-space extension setup can be easily transformed into the fibre extension version. To do this the two magnetic bases, each holding a prism mirror, are removed from the setup and a pair of fibre collimators are inserted. After successfully aligning the collimators, alignment tabs can be placed against the collimators to minimise the alignment procedures required when they are next removed from and re-added to the setup. Loops of optical fibre can be used to complete the optical path between the two collimators, where any length of fibre above ~ 10 cm can be chosen to create the desired OPD. These setups allow for a minimum OPD of 700 ps, measured using narrow width optical pulses.

To achieve an OPD less than this, the free-space extension depicted in figure 3.6 can be implemented. This setup can achieve an OPD ranging from 390 ps to 720 ps and consists of four prism mirrors, including the retroreflecting element. As this is a compact optical setup, there is not enough space to accommodate the SBC. However, as the setup is purely free-space optics, a quarter waveplate is included to create the necessary phase delay between the slow and fast polarisations of the reference signal.

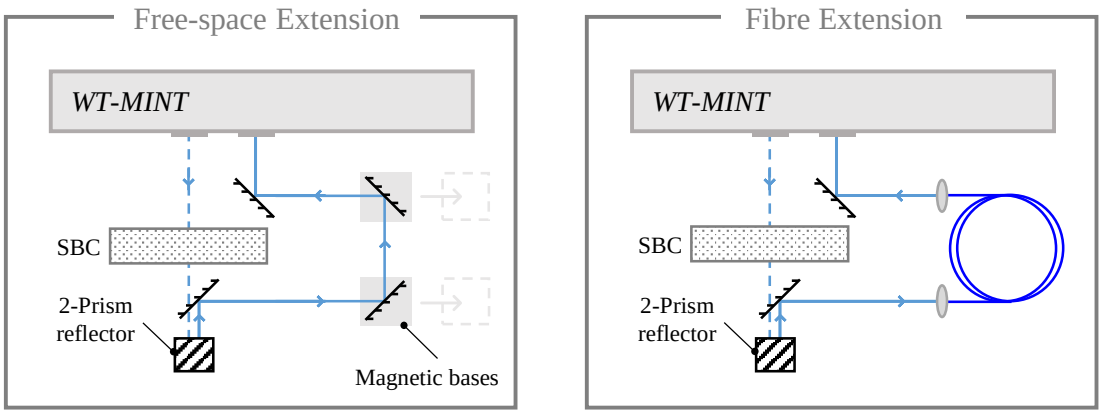


Figure 3.5: Schematics of the free-space and fibre extensions to the OPD of the AMZI. The schematics are top-down views of the setups, consisting of externally reflecting right-angle prism mirrors, magnetic bases, optical fibre (dark blue loops) and fibre collimators (grey ovals). The light-blue line shows the free-space beam path, where the dashed line is in a higher vertical plane compared to the rest of the beam path. The 2-prism reflector displaces the beam path in the vertical plane to accommodate the vertical separation of the WT-MINT outputs. The SBC is included in these setups. In the free-space setup, the magnetic bases, each holding a prism mirror, can be moved (as shown) to vary the optical path length of the external arm.

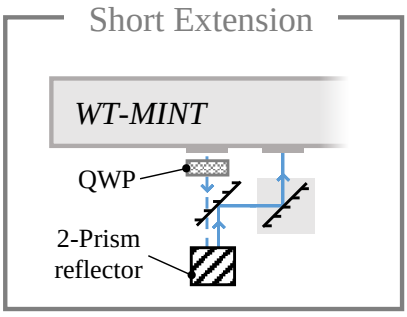


Figure 3.6: Schematic of the short free-space extension that allows OPD's between 390 ps and 720 ps to be achieved. The schematic is a top-down view of the setup, consisting of right-angle prism mirrors; including the 2-prism reflector. The light-blue line shows the free-space beam path, where the dashed line is in a higher vertical plane compared to the rest of the beam path. The SBC cannot be accomodated in this compact setup and is therefore replaced by a quarter waveplate (QWP).

3.1.2 Reference Signal Preparation & Detection

For the reference signal to perform the functionality described in section 2.5, the laser light must be prepared appropriately. Its polarisation state must alternate between the two orthogonal polarisation states aligned to the slow and fast axis of the PM fibre inputs to the AMZI. The optical power of the signal must also be adjustable, so that it can be balanced to provide the best feedback signal to the stabilisation system whilst reducing crosstalk with the single-photon level QKD signal. The reference signal is prepared using the setup shown in figure 3.7. Laser light, with a known wavelength-stability, is sent through an isolator and a variable optical attenuator to a switch, which directs the light down one of two paths. One path consists of a linear polariser that generates laser light aligned to the slow axis. The other consists of a linear polariser and an optical fibre that is keyed to the slow axis on one end and the fast axis on the other, therefore producing light aligned to the fast axis. Both the slow and fast signal arms are then combined using a PM coupler, where operation of the switch allows for the slow and fast polarisations of the reference signal to be sent alternately (not at the same time). One output of the PM coupler is sent to a monitoring power meter and the other output is sent towards the AMZI reference signal input, *InR*. The isolator is included to block any QKD signal that may propagate towards the reference laser, avoiding any interference with the lasing process and improving the reference signal's stability. Detection of the reference signal simply consists of a power meter at the output *OutR* of the AMZI. There is no need to extract the QKD signal from the detected reference signal, as the optical power of the reference light will be much brighter than the single-photon level QKD signal.

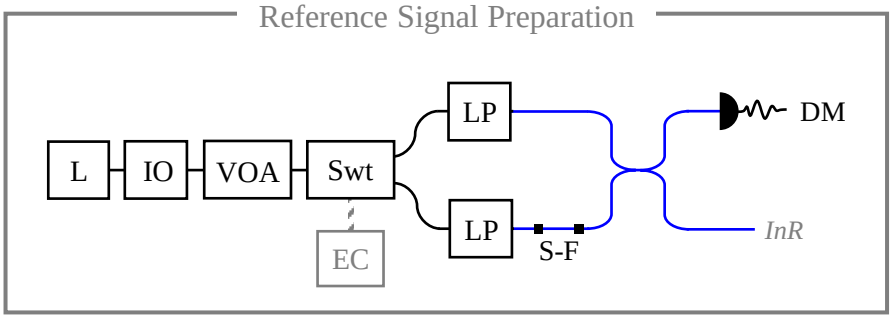
3.2 Measurement Procedure and Software Control

The measurement system incorporates many electronic devices that must be controlled and their inputs and outputs recorded. This includes all of the optical detectors, actuators for stages and the piezo and the optical switch for the reference signal preparation. To control the measurement system and record data for a characterisation measurement, a LabVIEW control program is developed, which controls, monitors and records all of the required parameters. The code also incorporates other functionality including data analysis, which, depending on the chosen measurement procedure, may be utilised to calculate the measured phase in real time. This section explores the main elements of the control code.

3.2.1 Procedures for Post-processing and Real-time Processing

Generally the measurement procedure for phase characterisation requires a phase sweep or multiple phase sweeps of the AMZI, which can be achieved using the piezo element incorporated in the WT-MINT. This produces interference patterns for both the reference and the QKD signal, from which the phases of these signals can be calculated. For measurement procedures that involve post-processing of the data, simply recording the detected optical powers is sufficient, from which the phases can be calculated after the experiment. This allows for a more accurate measurement of phase as complex analysis procedures can be executed, for example interpolation of peaks and troughs, selection of the closest peak and trough and selection of the slow or fast reference signal to minimise measurement uncertainty. See section 3.3.2 for further details.

Post-processing procedures are experimentally easier to implement when compared to real-time processing, but do not offer as much functionality. Real-time processing involves calculating the phase from the measured optical powers during the measurement procedure, which requires calibration steps prior to the experiment and produces a less



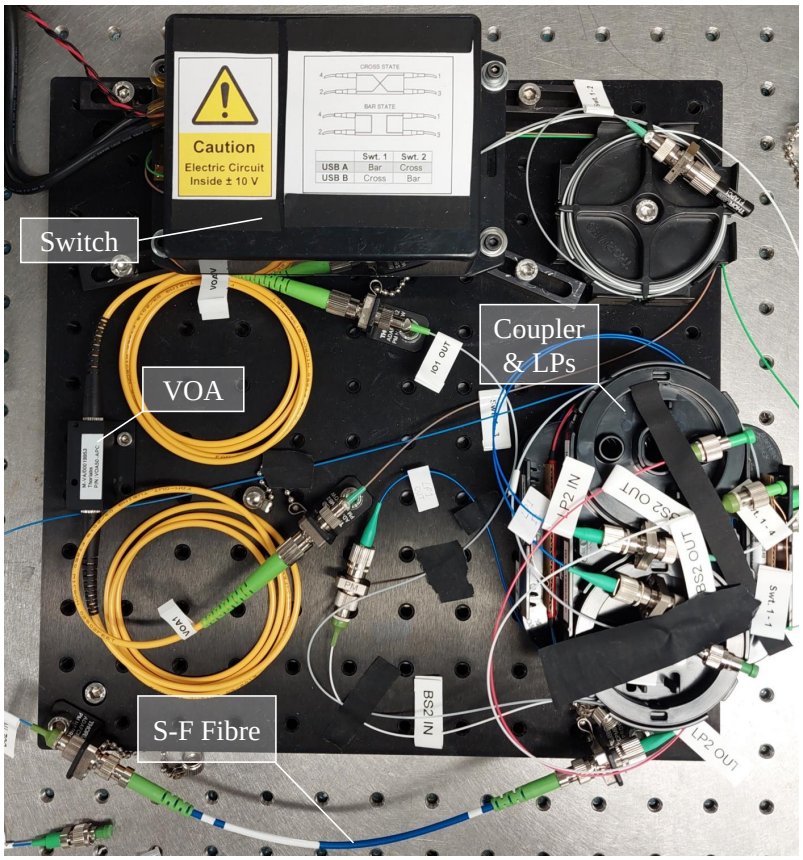


Figure 3.7: A schematic and photograph of the setup used to prepare the reference signal, consisting of the laser source (L), isolator (IO), variable optical attenuators (VOA), switch (Swt), linear polarisers (LP), PM 50:50 coupler and the monitoring detector (DM). The fast-aligned polarised signal is generated using a PM fibre patch cord that is keyed to the slow axis on one end and keyed to the fast axis on the other end (S-F). The switch element is electronically controlled (EC).

Basic Code Functions	**General Hardware Controls**	**Calibration Routines**	**Measurement Functions**
Initialise Idle Refresh Save Close	Piezo Stage SBC Polarisation-Switching	Pulse Overlap Min-Max Sweep Calculate & Set the Phase Offset	Determine Edge-Type (RT) Monitor $\Delta\theta_{IntR}$ (RT) Lock to Setpoint (RT) Read

Table 3.2: List of functions in the control software for the measurement system, grouped into the four described categories. The (RT) mark indicates that these functions are required for real-time processing.

accurate measure of the phase. However, this approach allows for operations such as phase locking, where a software-based PID loop is used to fix the phase difference between the arms of the AMZI by operating the piezo in response to environmental changes.

3.2.2 Software Control Overview

The measurement system is controlled via a LabVIEW program, which uses the queued message handler architecture [2], which consists of an event handling loop and a message handling loop. In response to user inputs, the event handling loop produces a message that is then queued, and the message handling loop constantly reads the queue and executes the enlisted messages. This architecture allows for the program to easily accommodate the controls required for the many pieces of hardware included in the measurement system, as well as allowing the complex functionality, particularly needed for real-time processing, to be incorporated. Screenshots of the front panel and block diagram [3] of the main program are shown in the appendix C.1, as well as the lists of operations performed by the event handling loop and the message handling loop.

The software is designed to consistently acquire the optical power readings from the measurement system, so that changes in the interferometer phase can be continuously monitored whilst performing other functions such as phase sweeps. The functions of the control software can be categorised into four sections, basic code functions, general hardware controls, calibration routines and measurement functions. The basic code functions are the base elements of any code, including the initialisation of hardware and the saving of data. General hardware controls concerns the individual operation of the instruments within the system, for example changing the voltage applied to the piezo. Calibration routines are particular sets of code that must be performed prior to the characterisation measurement to assess the state of the system and to extract the necessary parameters for calculations and feedback systems. Finally, the measurement functions are subroutines that are used to perform the characterisation measurement. A summary of the software for each of these categories is shown in table 3.2. Details of some of these functions are given in the following sections.

[2] Description of the queued message handler architecture can be found at [67]
[3] Descriptions of a LabVIEW software front panel and block diagram can be found at [68, 69]

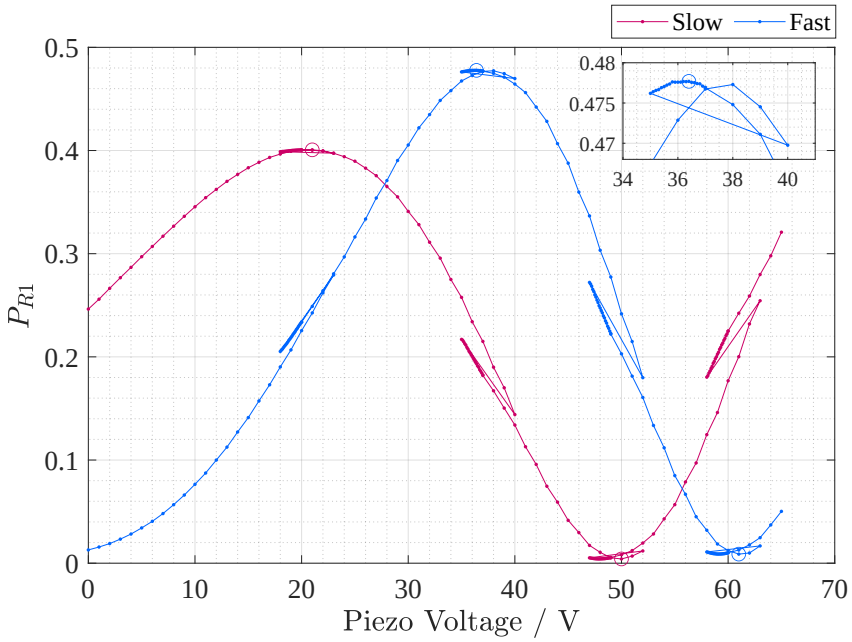


Figure 3.8: Power ratio, P_{R1}, between the detected output power and the monitoring power for both the slow and fast polarisation states of the reference signal, whilst varying the piezo voltage from 0 V to 65 V. The sweep is performed predominantly in incremental steps of 1 V, apart from over the peaks and troughs of the interference patterns, where the voltage is set back five steps and a re-sweep of the peak/trough is performed for increments of 0.1 V. Some evidence of hysteresis in the piezo element can be seen. For each setting of the piezo voltage, the power readings for both the slow and fast polarisation states are taken. The minimum and maximum values of the patterns are identified with a circle and the inset plot shows a magnification of the peak of the fast interference pattern.

3.2.3 Calibration Routines

Min-Max Sweep

The min-max sweep involves changing the phase difference between the arms of the AMZI using the piezo element. This produces an interference pattern for the reference signal, which can be used to extract the minimum and maximum values of the power ratio P_{R1}; the optical power at the interferometer output divided by the input power recorded by the monitoring detector as defined in equation 2.14 in chapter 2. This can in turn be used to calculate the interferometer phase. To perform the min-max sweep, the software varies the voltage applied to the piezo element in incremental steps of 1 V, which can be performed in a relatively short period of time ($<$ 1 minute). To ensure an accurate reading of the minimum and maximum value of the power ratio, the software detects when it has just passed over a region containing a peak or a trough in the interference pattern and jumps the voltage back five settings and re-sweeps the area with a smaller incremental step of 0.1 V. This results in power ratio traces like those shown in figure 3.8.

To obtain the interference patterns for both the slow and fast polarisation states of the reference signal, for each setting of the piezo voltage the polarisation state of the signal is switched and optical power readings for both states are recorded. The optical power readings are sorted for each polarisation state and the maximum and minimum of the power ratio is recorded and used for the phase calculations in the rest of the measurement procedure.

Calculate & Set the Phase Offset

As part of the min-max sweep the value of the phase offset, ψ_{off}, the phase difference between the slow and fast polarised interference patterns of the reference signal, can be measured and set. See section 3.3.2 for details on the definition of ψ_{off}. To set the phase offset, the software controls the actuator used to adjust the SBC, therefore changing the difference in phase delay imparted by the SBC onto the two polarisation states. To measure the phase offset, at the peak and trough of the slow polarisation pattern, the code determines the phase value of the fast polarisation state and calculates the difference between the two polarisation states. The code also does this for the peaks and troughs of the fast polarisation pattern and the average of the resulting four calculated values for the phase offset is taken to be ψ_{off}.

3.2.4 Measurement Functions

Determine Edge Type (real-time)

To unwrap the phase difference between the arms of the AMZI from $\psi_{IntR\,[0,\pi]}$ (equation 2.38) to $\psi_{IntR\,[0,2\pi)}$ (equation 2.39), it is necessary to determine the type of fringe edge that the interferometer is on, either falling or rising. For increasing OPD between the interferometer arms, the fringe edge is defined as falling if the output power decreases and the edge is defined as rising if the output power increases.

This functionality is typically not critical for post-processing procedures where a phase sweep is involved, as the piezo voltages are recorded with the detected optical powers, such that edge type can be determined after the fact. However, for real-time processing functionality, it is important to determine the edge type to calculate the phase during the measurement. To achieve this the piezo voltage is stepped by a small increment in the positive and negative direction, typically ± 0.5 V, and the resulting variation in the power ratio can be used to determine the edge type.

Monitoring $\Delta\theta_{IntR}$ (real-time)

This function allows the software to monitor the total change in the interferometer phase, $\Delta\theta_{IntR}$, over the course of a measurement. To do this, the phase change in either the slow or fast reference signal is calculated and the change in phase is accumulated for each recorded data point. The signal used, slow or fast, is chosen based on which signal is most sensitive and therefore effective at providing feedback for the current asymmetry of the interferometer. The reference signal is most sensitive when on the steepest part of the interference fringe, where the slow and fast fringes are offset from one another by ψ_{off} to improve measurement sensitivity over all values of θ_{IntR}. Figure 3.9 depicts the offset slow and fast polarised interference patterns and indicates the sensitive regions of the fringes that are effective for use in the calculation of $\psi_{IntR\,[0,\pi]}$. The limits of the effective regions of each polarisation of the reference signal are calculated using the value of ψ_{off} in the calibration stages of the measurement. If the OPD changes such that one of these limits is crossed, i.e. moving outside the effective region of one of the reference signal polarisations, the software is able to switch to the alternate polarisation state and use this to monitor the value of $\Delta\theta_{IntR}$.

Lock to Setpoint (real-time)

The lock to setpoint function uses the detected optical powers of the reference signal to determine the interferometer phase in the range $[0, \pi]$, $\psi_{IntR\,[0,\pi]}$, and uses the piezo element to minimise deviations from this setpoint. A software PID loop with adjustable

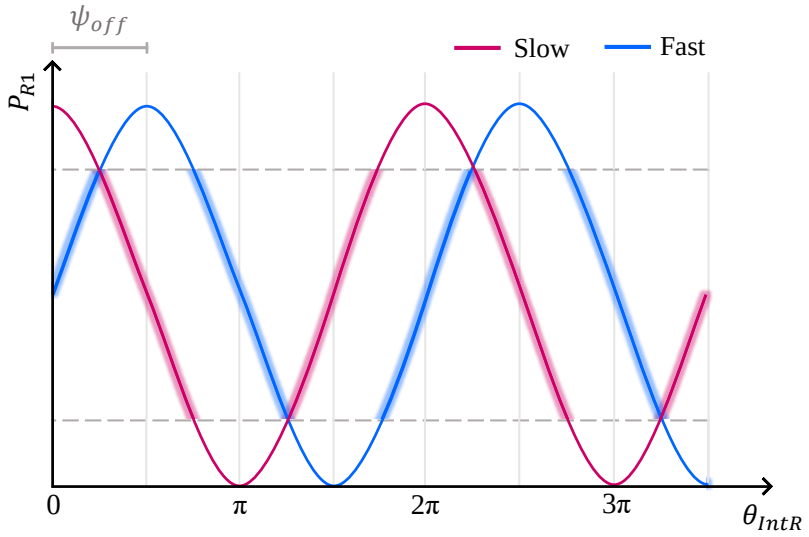


Figure 3.9: Schematic showing the power ratio P_{R1} for the slow and fast polarisations of the reference signal that are offset by ψ_{off}. The regions of these two signals that can be used effectively to provide sensitive feedback on the phase difference of the interferometer are highlighted.

values for the proportional, integral and differential settings is used to determine the feedback response, and either of the slow or fast polarisations of the reference signal can be used as feedback. Data demonstrating the locking functionality of the measurement system is shown in section 3.3.3.

3.3 Preliminary Testing of the Measurement System

To assess the functionality of the measurement system and test the software control code described in the previous section, preliminary experimental tests of the primary elements of the system are performed. The system components of particular interest are the WT-MINT stage, used for pulse overlap adjustment, the piezo element, used for phase sweeps, the stability of the AMZI for different lengths of OPD and the single-photon detection of the QKD signal.

3.3.1 WT-MINT Stage

The stage element of the WT-MINT allows the interferometer OPD to be adjusted to achieve accurate overlap of the incoming optical pulses. The stage element is specified to have a delay range of 0 to 300 ps ($\equiv$ 9 cm) and a minimum incremental step size of 3 fs ($\equiv$ 900 nm) [63]. The stage element affects the optical path length (OPL) of the internal arm of the AMZI. To test the delay range of this element, bright laser pulses are sent into the measurement system for various settings of the WT-MINT. This signal is generated using a PicoQuant LDH-P-F-N-1550 laser head [70] controlled by a PDL 800-D [71] picosecond laser diode driver, with a wavelength of 1549.5 nm, a pulse full width half maximum of $\sim$ 150 ps and a pulse repetition rate of 40 MHz. The signal is detected using a Thorlabs DXM30AF fast photodode [72] and an Agilent Infiniium DCA-J 86100C sampling oscilloscope.

Firstly the WT-MINT tap is disabled, where the mirrors of the WT-MINT are retracted, such that the external beam does not exit the WT-MINT housing. The internal

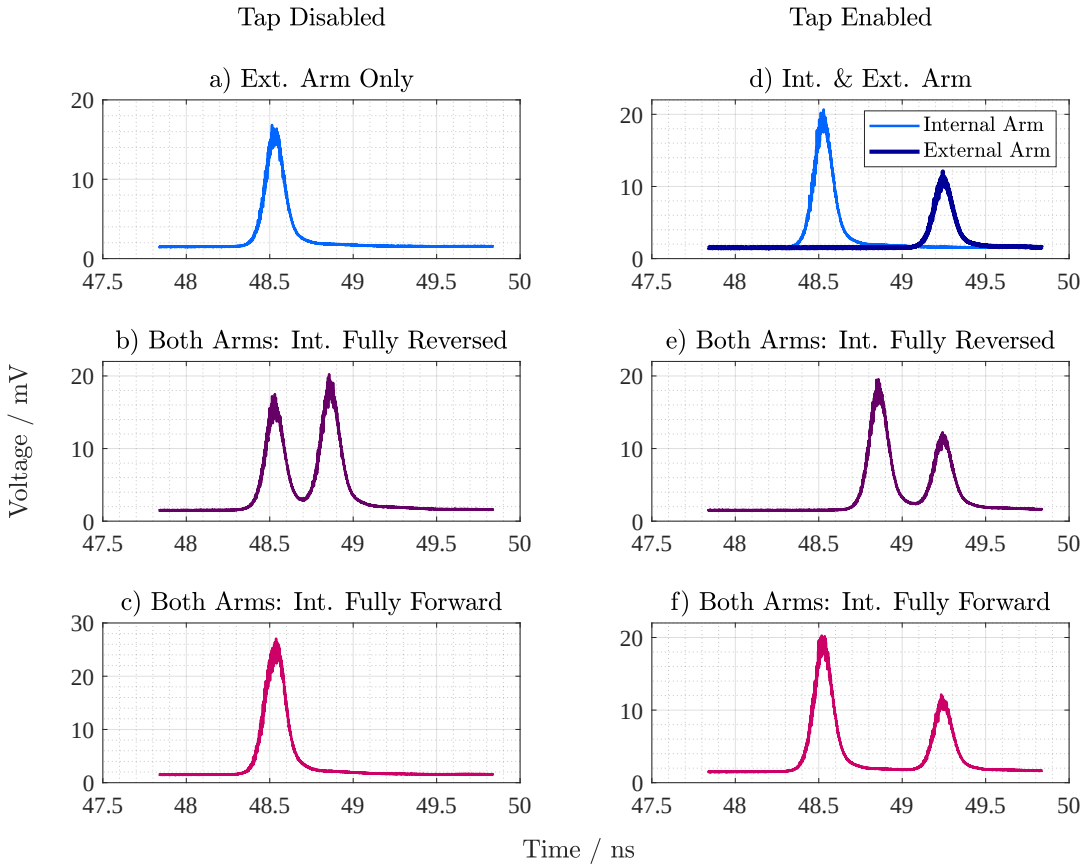


Figure 3.10: Traces of optical pulses that have passed through the measurement system for various settings of the WT-MINT. The tap disabled and enabled settings correspond to the position of the retractable mirrors in the WT-MINT, the fully reversed or forward terms refer to the setting of the delay stage element and the internal (Int.) and external (Ext.) arms of the interferometer are sometimes blocked to allow the pulses corresponding to each path to be identified.

arm of the AMZI is blocked using the attenuator element of the WT-MINT, allowing the pulses to propagate through the external arm only. The resulting trace is shown in figure 3.10a), allowing the pulses corresponding to propagation through the external arm to be identified. The internal arm is unattenuated and the stage element is set to its fully reversed position, producing the trace shown in figure 3.10b). This trace indicates an OPD of 330 ps for the fully reversed setting. Figure 3.10c) is produced when the stage is set to its fully forward setting, where the pulses propagating through the internal and external arm fully overlap, indicating no OPD. Therefore, when the tap is disabled, the stage can adjust the OPD from 0 to 330 ps, greater than the 300 ps specified range.

The TAP is then enabled and the retractable mirrors are positioned to reflect the external beam out of the WT-MINT housing. The external beam was sent into a free-space extension with a delay length of $\sim$ 400 ps, after which it was directed back into the WT-MINT. Figure 3.10d) shows the detected optical pulse traces corresponding to propagation through the internal arm and the external arm of the AMZI. The internal arm trace is achieved by blocking the the external arm of the AMZI and the external arm trace is achieved by using the attenuator element to block the internal arm. This allows the pulses corresponding to propagation through each arm to be identified. The trace in figure 3.10e) is the result of allowing the pulses to propagate through both the internal arm and the external arm and setting the WT-MINT stage to its fully reversed position.

Figure 3.10f) shows the same, but with the stage set to its fully forward position. The resulting OPD range is 390 ps (fully reversed) to 720 ps (fully forward).

To assess the minimum incremental step of the WT-MINT stage, it was not necessary to characterise the value of the incremental change in the OPD, but instead to ensure that this incremental change is less than half of the reference signal wavelength $\lambda_R/2 = 771$ nm ($\equiv 2.57$ fs). To assess this, CW laser light at λ_R was sent into the WT-MINT and the stage settings were adjusted. The light was detected using photodiodes, where the voltage response of these diodes was recorded using a high sampling rate voltmeter. The stage has two settings, speed and step size, where each of these settings are given in arbitrary units. The speed was set to its lowest value, 1, and the step size was adjusted for values between 8 and 96. The resulting voltage traces of the detected CW signal for steps made at varying step increments are shown in figure 3.11. The traces show the resolved steps, where it is clear that the minimum step size of 8 is contained within one fringe. Therefore, the minimum step size is much shorter than half a wavelength of the reference signal and, additionally, step sizes of 32 and greater result in OPD changes larger than one reference signal wavelength.

3.3.2 Piezo Element

The piezo element within the WT-MINT allows for adjustments to the OPD on the sub-wavelength scale and can be used to perform phase sweeps producing interference patterns for the reference and the QKD signal. To demonstrate this, CW laser light is generated using a Rio Orion laser [73], with a peak wavelength of 1542.1 nm, and is sent through the WT-MINT and detected using a power meter. A piezo controller is used to apply a voltage to the piezo element, and the voltage setting is varied between 0 V and 70 V in incremental steps of 0.1 V. Figure 3.12 shows the resulting interference patterns for both the slow and fast polarisation states of the reference signal. For each setting of the piezo voltage, the input polarisation state of the reference signal is alternated, so that an optical power reading can be taken for both polarisation states.

The interference pattern resulting from the piezo sweep clearly indicates that interference is occurring and can be utilised when performing other procedures, such as fine tuning the pulse overlap, where visible constructive and destructive interference indicates that good pulse overlap has been achieved. Performing a piezo sweep is critical to the phase measurement procedure, as it allows the minimum and maximum power ratio of the interference pattern to be found, which in turn allows for the detected optical powers to be converted into a phase value.

Identifying P_{Rmax1} & P_{Rmin1}

To calculate the interferometer phase from the reference signal, $\psi_{IntR\,[0,\pi]}$, the maximum and minimum value of the power ratio P_{R1} in the interference pattern must be identified (P_{Rmax1} and P_{Rmin1}), as defined in equations 2.17 and 2.18 for a detector D1. To do this, the data points taken from a phase sweep, like that shown figure 3.12, can be used to determine the values of P_{Rmax1} and P_{Rmin1}. As the 0.1 V incremental sweep in figure 3.12 shows good resolution of the peaks and troughs, the maximum and minimum values for the power ratio can be extracted from the data points directly, by simply finding the maximum and minimum values. However, as a 0.1 V increment piezo sweep between 0 V to 70 V typically takes $\sim$ 13.5 minutes to complete, this type of sweep may not be appropriate for all measurement scenarios.

In these cases, a 1 V increment sweep is performed, however this does not provide an appropriate resolution of the peaks and troughs to provide a good estimate for the value of P_{Rmax1} and P_{Rmin1}. Therefore, the peaks and troughs for these sweeps are interpolated

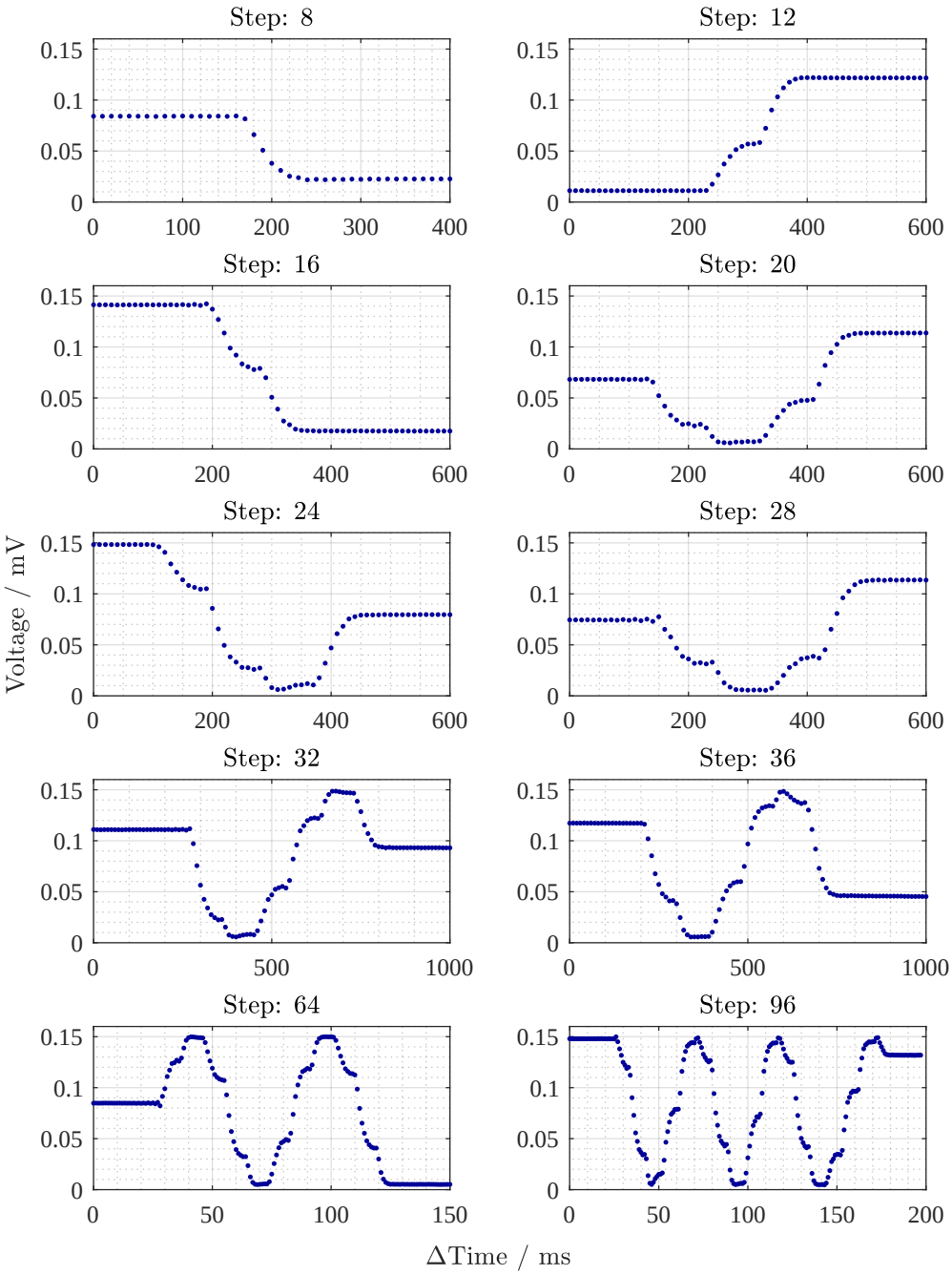


Figure 3.11: Voltage traces of the detected CW optical signal from the measurement system for incremental changes to the stage element of varying step sizes.

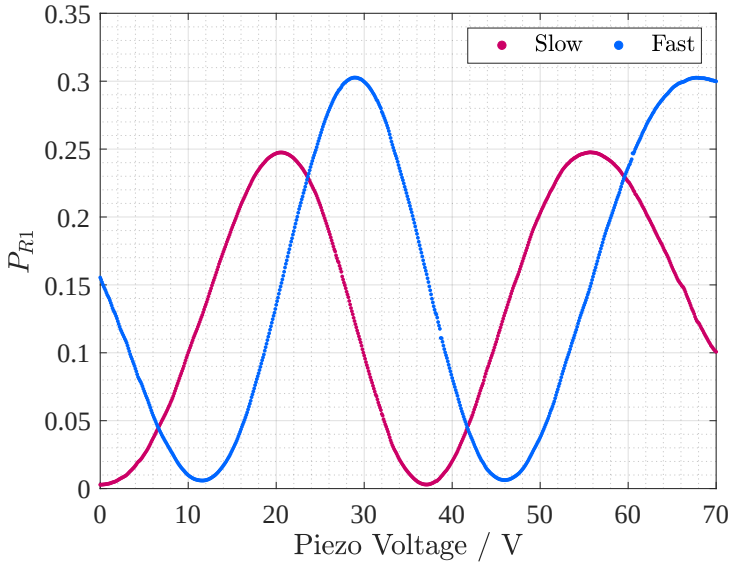


Figure 3.12: Resulting power ratio P_{R1} interference patterns of the reference signal for both the slow and fast polarisation states when the voltage applied to the piezo element is varied between 0 V and 70 V.

by fitting a parabola to the four data points closest to the peak/trough. The justification for this is explored in appendix C.2.

Calculating Phase

Taking the interference patterns resulting from the phase sweep shown in figure 3.12, the change in the phase difference between the arms of the AMZI can be calculated. The interference patterns and the resulting phase changes for the different ranges ($\psi_{IntR\,[0,\pi]}$, $\psi_{IntR\,[0,2\pi)}$ and θ_{IntR}) are shown in figure 3.13. Equations for $\psi_{IntR\,[0,\pi]}$ and $\psi_{IntR\,[0,2\pi)}$ are given in section 2.4.1, where the edge type of the fringe must be known to unwrap from the $[0,\pi]$ range to the $[0,2\pi)$ range. For a piezo sweep, determining the edge type is straightforward, as the piezo voltage is positively correlated with the OPD, therefore the edge type can be determined by observing the change in the value of P_{R1} with the piezo voltage. From equation 2.39, the value of $\psi_{IntR\,[0,2\pi)}$ can be more explicitly written as,

$$\text{Rising Edge:} \quad \psi_{Int\,[0,2\pi)} = \psi_{Int\,[0,\pi]} \qquad (\text{mod } 2\pi) \tag{3.1}$$

$$\text{Falling Edge:} \quad \psi_{Int\,[0,2\pi)} = 2\pi - \psi_{Int\,[0,\pi]} \qquad (\text{mod } 2\pi). \tag{3.2}$$

As the piezo voltage sweep between 0 V to 70 V progresses in one direction, the fully unwrapped interferometer phase $\Delta\theta_{IntR}$ can be calculated from $\Delta\psi_{Int\,[0,2\pi)}$. This is done by determining the direction of the voltage sweep, which in this case is negative (from 70 V down to 0 V), and performing the following equation,

$$\Delta\theta_{Int\,i} = \Delta\psi_{Int\,[0,2\pi)\,i} \pm 2\pi N \tag{3.3}$$

where i is the data index, N is the number of peaks that have been traversed to reach data point i in the sweep and the $\pm$ sign is chosen depending on the direction of the sweep. The value of the fully unwrapped phase change $\Delta\theta_{IntR}$ for the slow and fast polarisations can be used to calculate the phase offset, ψ_{off} for the reference signal,

$$\begin{aligned} \psi_{off} &= \theta_{IntS} - \theta_{IntF} && (\text{mod } 2\pi) \\ &= \Delta\theta_{IntS} - \Delta\theta_{IntF} && (\text{mod } 2\pi). \end{aligned} \tag{3.4}$$

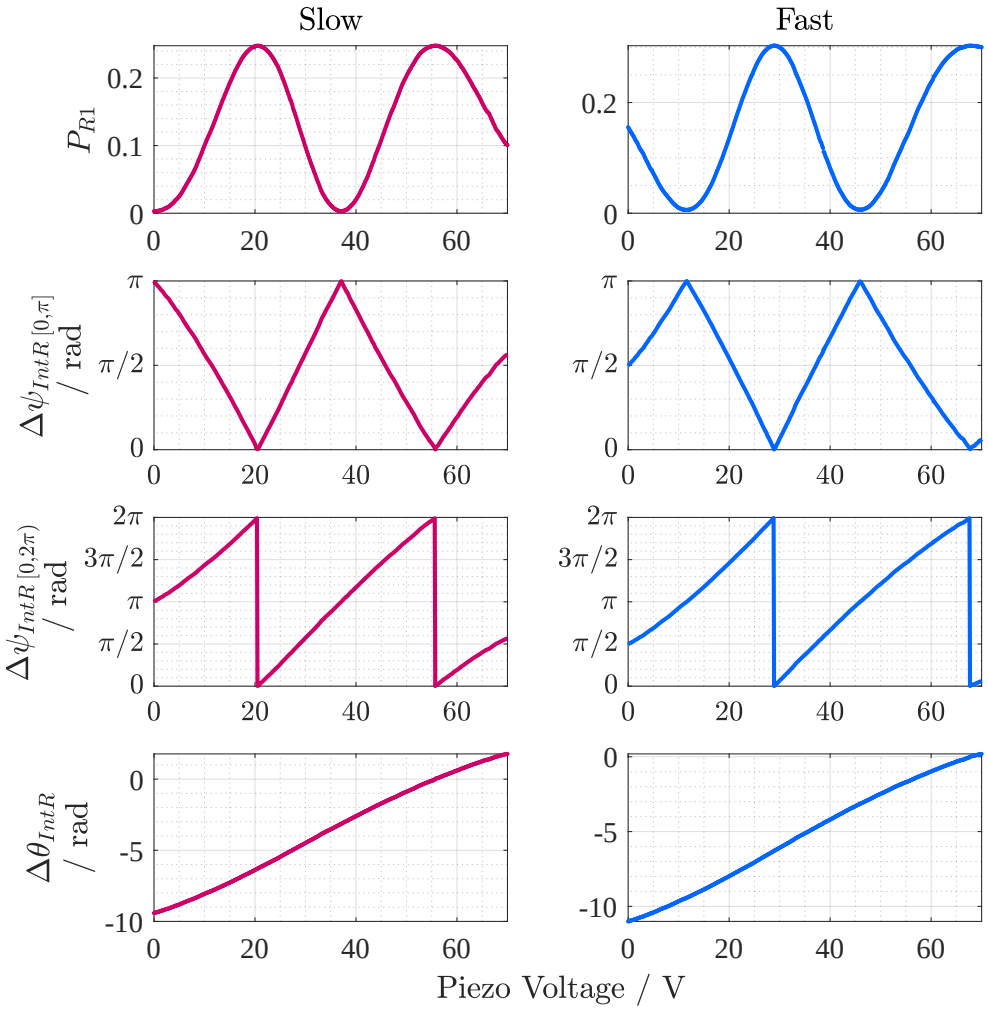


Figure 3.13: Plots of the power ratio, P_{R1}, interference patterns for the slow and fast polarisations resulting from a piezo sweep between 0 V and 70 V (top). Below this are plots for the corresponding change in the interferometer phase bound between $[0, \pi]$, $\Delta\psi_{IntR\,[0,\pi]}$ (second from top), the change in the interferometer phase bound between $[0, 2\pi)$, $\Delta\psi_{IntR\,[0,2\pi)}$ (second from bottom), and the fully unwrapped interferometer phase change, $\Delta\theta_{IntR}$ (bottom).

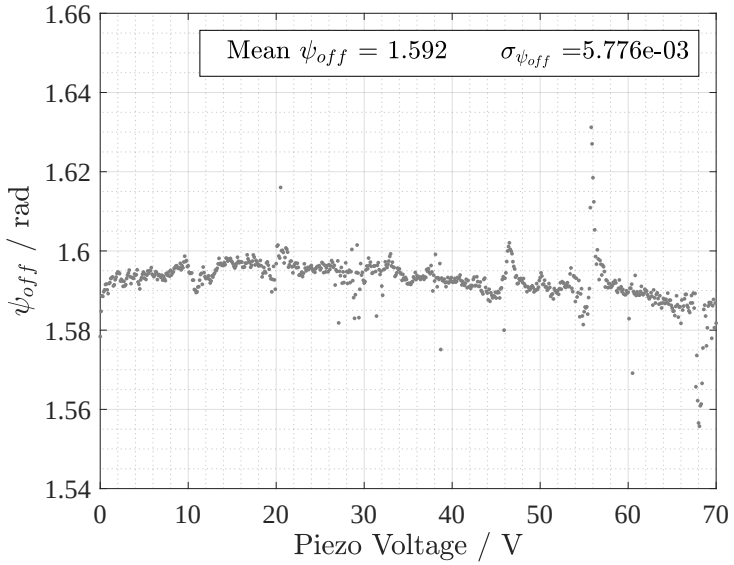


Figure 3.14: The phase offset, ψ_{off}, between the slow and fast polarised states of the reference signal, calculated from the values of the unwrapped phase change $\Delta\theta_{IntR}$ shown in figure 3.13. The mean phase offset and the standard error of the mean $\sigma_{\psi_{off}}$ are shown.

The phase offset is plotted in figure 3.14 for the interferometer phases shown in figure 3.13. The resulting total change in the interferometer phase for the piezo sweep calculated from the two reference signals shown in figure 3.13 are,

$$\begin{aligned} \text{Slow:} \quad & \Delta\theta_{IntS} = -11.1980 \text{ rad} \\ \text{Fast:} \quad & \Delta\theta_{IntF} = -11.1946 \text{ rad} \end{aligned}$$

which agree to within 4 mrad of each other. Given the wavelength of the reference signal is $\lambda_R = 1542.1$ nm, the total change in the OPD for the 70 V to 0 V piezo sweep is 2.746 μm.

Varying Peaks and Troughs

For the phase calculations detailed above, it is assumed that the maximum and minimum of the interference pattern, the values of P_{Rmax1} and P_{Rmin1}, are consistent over the course of a measurement. From the model explored in chapter 2, this is equivalent to assuming that, during the measurement, the following properties remain constant:

- The fibre coupler splitting ratios
- The detection efficiencies of the detectors
- The transmittance and reflectance of the AMZI beam splitters
- The loss in each arm of the AMZI
- The pulse temporal overlap

This results in the sum and difference terms, S_1 and D_1, being constant. However, using the piezo element to perform multiple short phase sweeps over the peaks and troughs of the interference fringe, it is shown that the values of P_{Rmax1} and P_{Rmin1} are not constant. Figure 3.15 shows the maximum and minimum power ratio data points taken from short

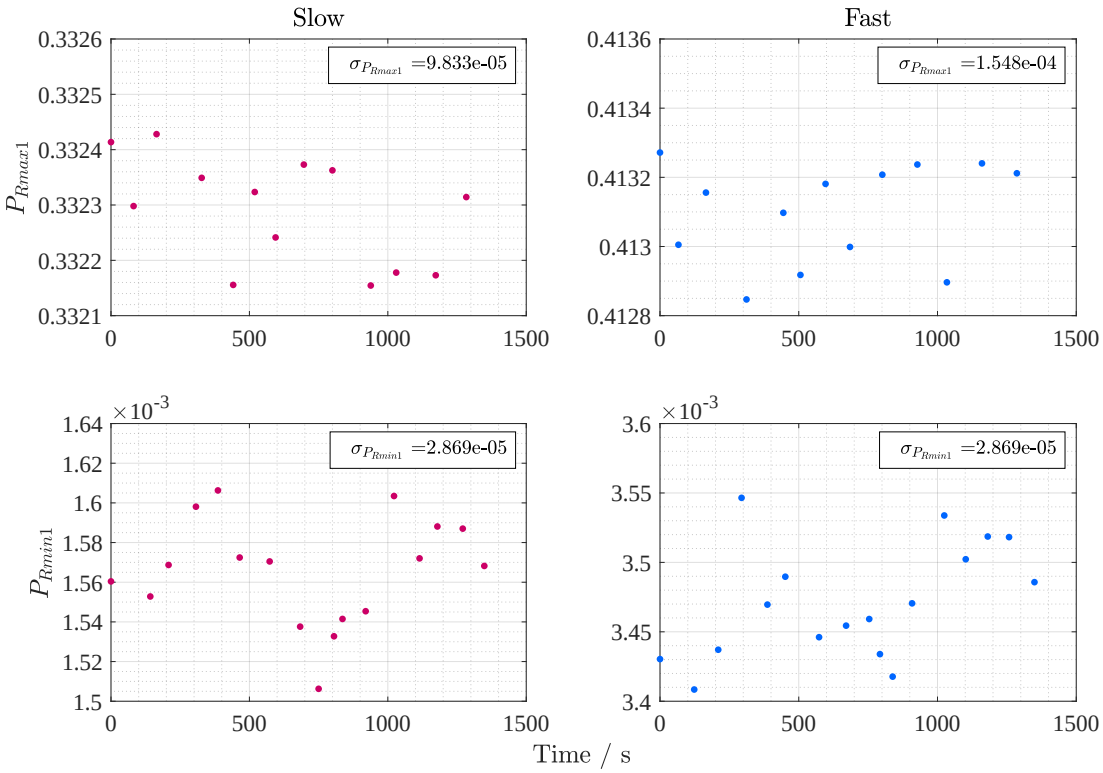


Figure 3.15: Plots of the maximum and minimum values of the power ratio, P_{Rmax1} and P_{Rmin1}. Values for both the slow and fast polarisations of the reference signal are shown. The data was collected by performing repeated short range 0.1 V increment piezo sweeps in the regions of a peak and trough of each interference pattern. The uncertainty of the mean for each dataset is calculated.

range 0.1 V increment sweeps of the piezo voltage in the local area of the peak and trough for the slow and fast polarisation signals of the reference laser. To account for this variation as best as possible, when calculating the phase from the recorded power ratio, for every data point the values of P_{Rmax1} and P_{Rmin1} nearest to that data point will be used to calculate the phase.

In addition to this, repeated sweeps of the WT-MINT piezo element revealed another feature; the transmittance of the AMZI arms varies with the piezo setting. To demonstrate this, the two polarisations of the CW reference signal (Rio Orion laser [73]) are sent into the AMZI, for three different formations of the measurement setup. In the first, the WT-MINT is tap-enabled with a free-space extension with an $OPD = 30$ cm. In the second, the WT-MINT is tap-enabled with a free-space and fibre extension with an $OPD = 7.66$ m and 5 m of optical fibre. In the final state the WT-MINT tap is disabled. The external arm of the AMZI is blocked, allowing light to only propagate through the internal arm, and the voltage applied to the piezo element is repeatedly swept between 0 V and 70 V. This is then repeated with the internal arm blocked, allowing light to propagate through only the external arm. For each voltage setting the input polarisation of the reference signal is switched and an optical power reading is made for both states. The monitoring power and the power at the output of the AMZI are recorded and used to calculate the percentage change in the power ratio of both the slow and fast polarisations of the signal. The percentage change is calculated as follows,

$$\frac{P_{R1} - \mu_{P_{R1}}}{\mu_{P_{R1}}} \times 100 \tag{3.5}$$

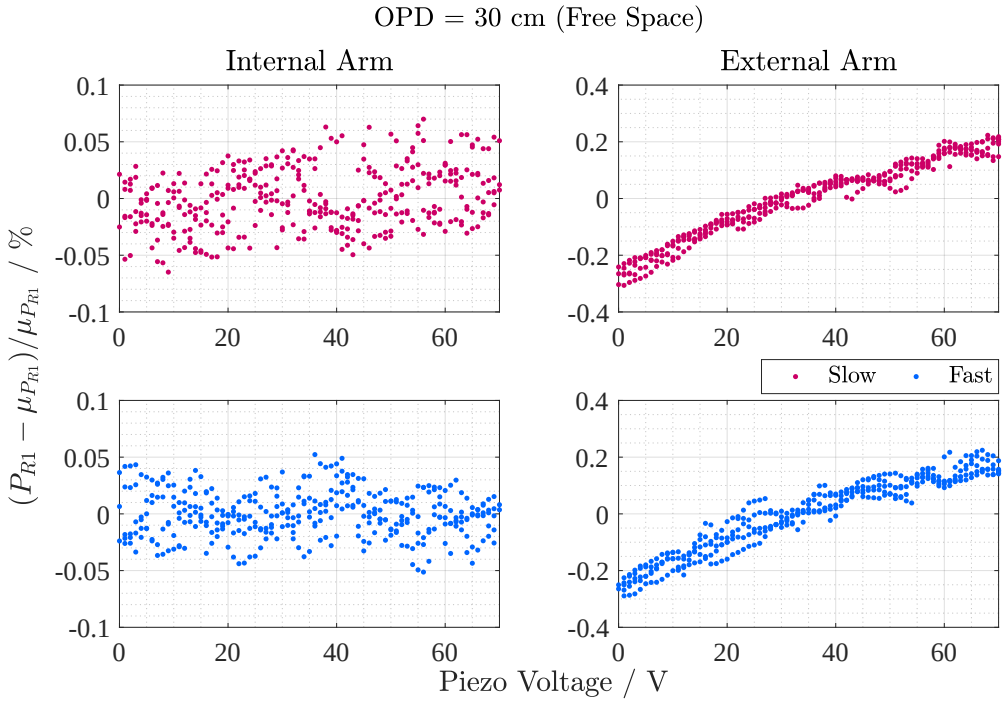


Figure 3.16: The percentage change of the power ratio for the slow and fast polarisations of the reference signal for changing piezo voltage when propagating through either the internal or the external arm of the AMZI. The WT-MINT is set to the tap-enabled state with a free-space extension and an $OPD = 30$ cm. The piezo voltage is swept between 0 V and 70 V 5 times.

where $\mu_{P_{R1}}$ is the mean power ratio. Figures 3.16 3.17 show the percentage change in the power ratio for the $OPD = 30$ cm tap-enabled case and the $OPD = 7.66$ m tap-enabled case. For the 30 cm free-space extension, the transmittance through external arm is positively correlated with the voltage applied to the piezo element, whereas the transmittance through the internal arm appears unaffected. Similarly for the 7.66 m fibre and free-space extension, the internal arm is unaffected by the piezo setting, however the transmittance through the external arm is negatively correlated. For the tap-disabled setting, only the internal arm could be blocked, and the resulting percentage change in the power ratio is shown in figure 3.18. The transmittance through the external arm is negatively correlated with the applied piezo voltage.

The changing value of P_{Rmax1} and P_{Rmin1} and the variation in the transmittance of the external arm must be accounted for in the uncertainty calculations for the reference signal interferometer phase. This is explored further in section 3.4.

3.3.3 Stability Tests for Different OPDs

To perform a basic assessment of the stability of the measurement system for different OPD settings, a series of measurements were conducted for both free-space and fibre extensions to the WT-MINT in the tap-enabled state. The OPD lengths tested were, $OPD = 35$ cm (no fibre), $OPD = 62$ cm (20 cm of fibre), $OPD = 1.2$ m (60 cm of fibre), $OPD = 1.5$ m (1 m of fibre), $OPD = 7.7$ m (5 m of fibre) and $OPD = 15$ m (10 m of fibre). The software-based PID loop described in section 3.2 is used to lock the interferometer to a phase difference set point of $\psi_{IntR\,[0,\pi]} = \pi/2$. The PID loop is then disabled and the drift in the interferometer phase is recorded. The detected optical powers are converted into the change in phase ($\Delta\psi_{IntR\,[0,\pi]}$) and the results are shown in figure 3.19 for the various

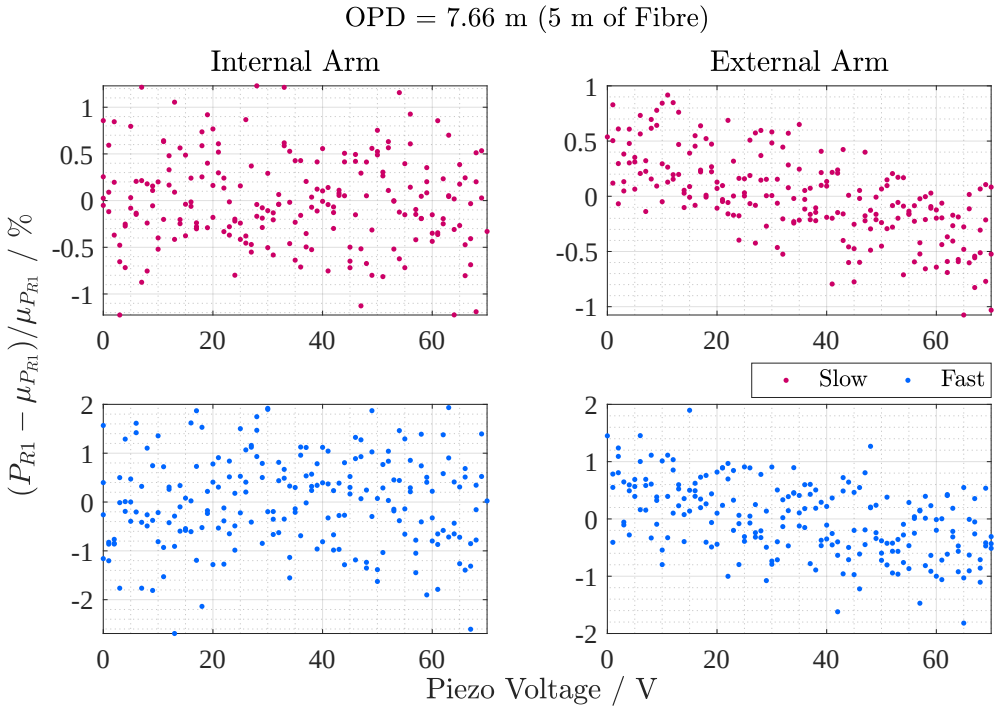


Figure 3.17: The percentage change of the power ratio for the slow and fast polarisations of the reference signal for changing piezo voltage when propagating through either the internal or the external arm of the AMZI. The WT-MINT is set to the tap-enabled state with a free-space and fibre extension and an $OPD = 7.66$ m (5 m of fibre). The piezo voltage is swept between 0 V and 70 V 3 times.

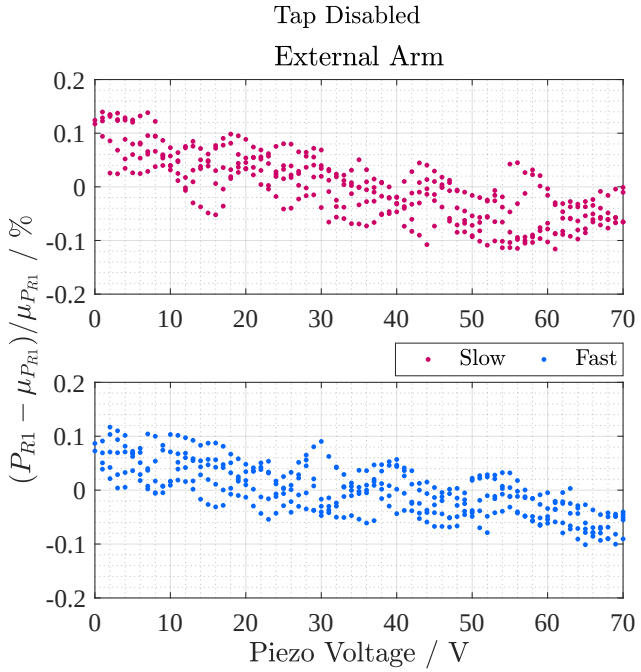


Figure 3.18: The percentage change of the power ratio for the slow and fast polarisations of the reference signal for changing piezo voltage when propagating through the external arm of the AMZI. The WT-MINT is set to the tap-disabled state and the piezo voltage is swept between 0 V and 70 V 5 times.

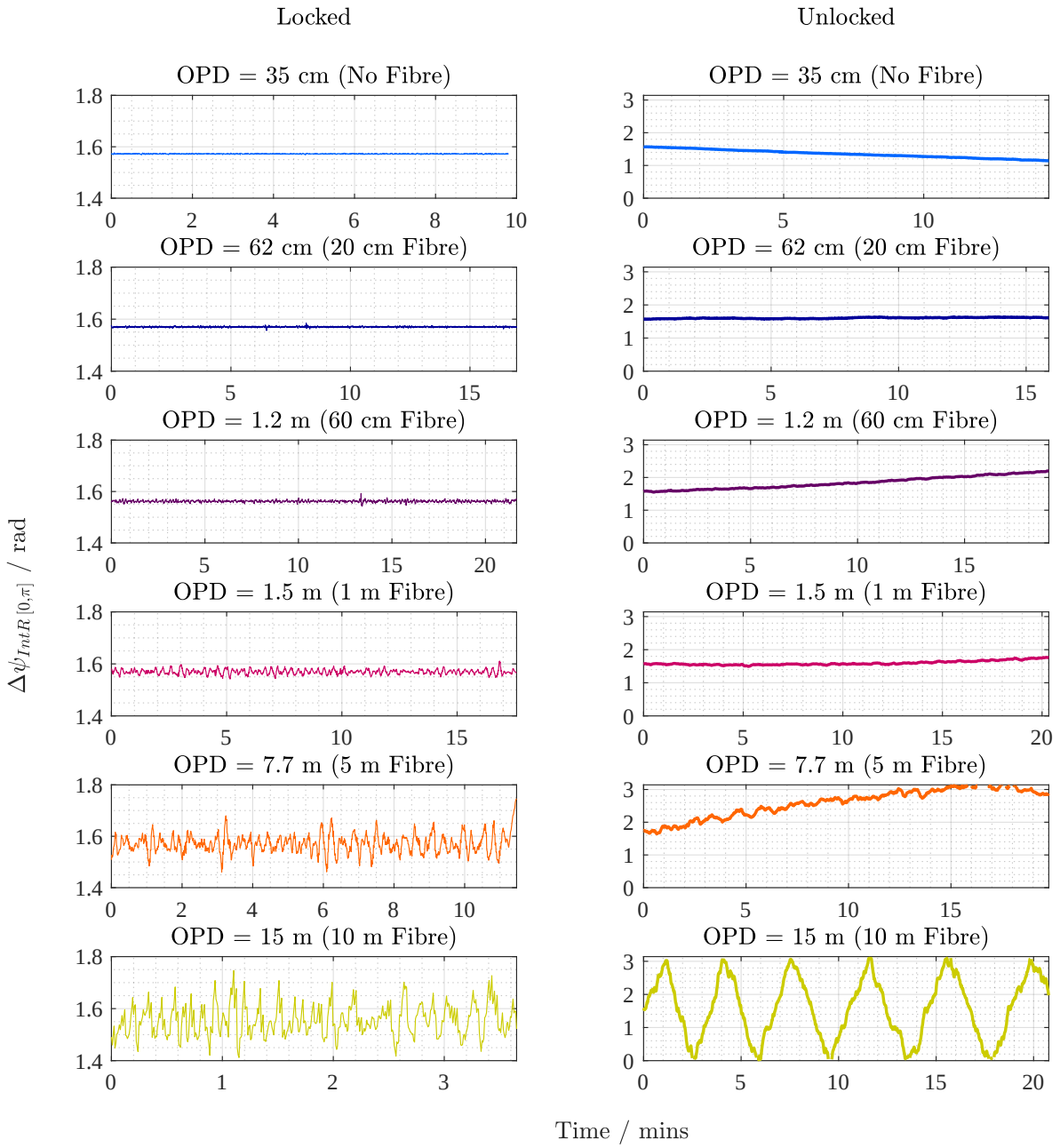


Figure 3.19: Change in the interferometer phase $\Delta\psi_{IntR\,[0,\pi]}$ for different configurations of the tap-enabled WT-MINT when the software-based PID loop is locked and subsequently unlocked.

configurations of the system.

The performance of the software-based PID loop is clearly demonstrated, where, as anticipated, the phase stability is improved for shorter OPDs of the AMZI. For the longer lengths of optical fibre, the drift of the OPD is more substantial, such that in some cases the locking was stopped early as the piezo voltage reached either its upper or lower voltage limit. Work was done towards implementing the stage element into the locking procedure to compensate for cases where the piezo voltage reached its limits, however further development is needed in this area. In the unlocked datasets the drift in the interferometer phase is affected by how long the measurement system is left to thermally settle after being setup. Therefore, in some cases, the drift is more significant for smaller OPDs compared to longer OPDs.

3.3.4 Single-photon Detection

Single-photon detection is performed using a gated ID210 by IDQuantique [74]. For most measurements the clock rate of the detector is set to be equal to the pulse repetition rate for that measurement, typically 40 MHz, and the dead time is set to be $\tau_{dead} = 40$ µs. This long dead time setting renders the afterpulse probability to be negligible [75] and results in a maximum count rate of $1/\tau_{dead} = 25$ kHz. Upon the detection of a photon, 40 µs worth of detection gates are rendered blind, such that they are not able to detect a photon. These gates are referred to as off gates, where the number of off gates is denoted N_{off}. When collecting many counts with an SPD to construct an interference pattern, the number of photons sent to the SPD will vary across the pattern, for example more photons will be sent at the peak of the interference pattern in comparison to the trough. As more photons are sent, the number of off gates will increase, restricting the number of photons that can be detected per second. Therefore the number of counts recorded by the SPD must be scaled according to the number of available detection gates, referred to as on gates. The number of on gates is denoted by N_{on} and is given by the following equation [41],

$$N_{on} = N_{clock} - N_{count}\lfloor \tau_{dead} N_{clock} \rfloor \tag{3.6}$$

where N_{clock} is the number of clock counts (the clock rate) of the SPD, N_{count} is the number of counts detected by the SPD and τ_{dead} is the dead time. The number of off gates is therefore given by [41],

$$N_{off} = N_{clock} - N_{on}. \tag{3.7}$$

For the detection of an interference pattern, to scale the number of counts appropriately, firstly the probability of correctly detecting a photon can be calculated [41],

$$p_{TC1} = \frac{N_{counts} - N_{DC}}{N_{pulses} - N_{off}} \tag{3.8}$$

where N_{DC} is the number of dark counts. This can be used to calculate the mean photon number per pulse using equation 2.24 restated here for convenience [41],

$$\mu = -\frac{1}{\eta_1} \ln\left(1 - p_{TC1}\right) \tag{2.24, revisited}$$

where η_1 is the detection efficiency of the SPD. To observe this scaling transformation between the detector counts N_{counts} and the mean photon number μ, highly attenuated pulses of light were interfered in the measurement system and the piezo element was swept between 0 V and 70 V. The resulting interference fringes in detector counts and in the mean photon number per pulse, as calculated by equation 2.24, are shown in figure 3.20.

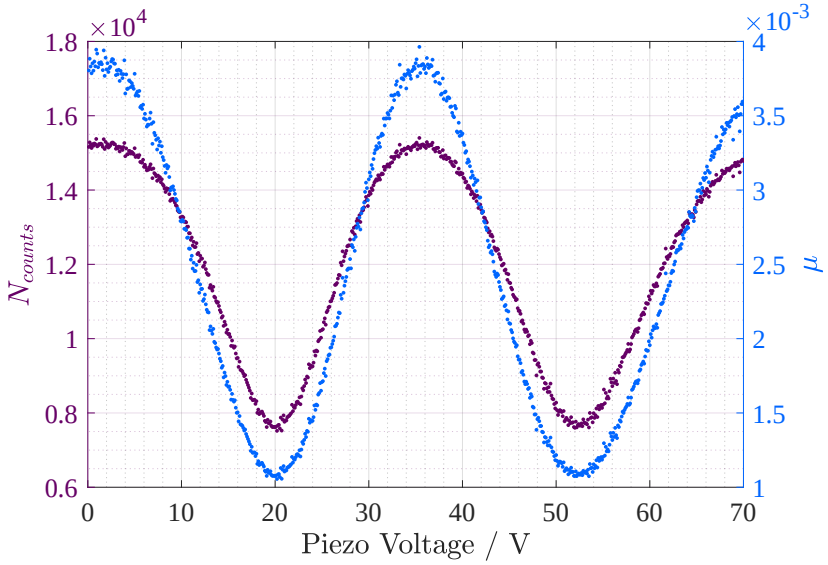


Figure 3.20: The number of SPD detected counts, N_{counts}, and the mean photon number per pulse, μ, for a piezo sweep of the measurement system.

The plots clearly show that the number of counts flatten at the peaks of the interference pattern compared to the troughs due to the reduction in gates available to detect incoming photons. Whereas, the scaled mean photon number per pulse value restores the symmetry between the peaks and troughs of the interference pattern. To assess the phase of the QKD signal detected by the ID210, the detector counts will be converted into the mean photon number per pulse, μ.

3.4 Phase Uncertainty Calculations

From the preliminary testing of the measurement system, it is clear that some elements of the system do not behave fully as anticipated as in the theory calculations explored in chapter 2. For example, variation in the optical transmittance with the piezo setting, variation in the maximum and minimum of the power ratio and general noise from the optical detectors. Therefore, it is necessary to introduce uncertainty calculations to account for these deviations to the model, resulting in an uncertainty on the final phase measurement of the QKD signal. In addition to this, the error terms from the phase conversion equation in section 2.4.3 can be incorporated into these uncertainty calculations. This section explores the propagation of uncertainty through the calculation of the unwrapped change in the interferometer phase from the reference signal, $\Delta\theta_{IntR}$. A simplified form of these uncertainty calculations can also be applied to the QKD signal phase calculation.

3.4.1 Uncertainty in $\Delta\psi_{IntR\,[0,\pi]}$ and $\Delta\psi_{IntR\,[0,2\pi)}$

Using equation 2.38, an estimate for the measurement uncertainty of $\psi_{IntR\,[0,\pi]}$ is given by,

$$\sigma_{\Delta\psi_{IntR\,[0,\pi]}} = \frac{-1}{\sqrt{1-u^2}}\sigma_u \tag{3.9}$$

where,

$$u = \frac{1}{D_{1R}}\left(S_{1R} - 2\frac{P_{1R}}{P_{MR}}\right) \tag{3.10}$$

$$\sigma_u = \frac{1}{D_{1R}^2}\left[\left(S_{1R} - 2\frac{P_{1R}}{P_{MR}}\right)\sigma_{D_{1R}} + D_{1R}\left(2\sigma_{P_{1R}/P_{MR}} + \sigma_{S_1R}\right)\right] \tag{3.11}$$

and $\sigma_{S_{1R}}$ and $\sigma_{D_{1R}}$ are the uncertainties in the sum and difference terms respectively and $\sigma_{P_{1R}/P_{MR}}$ is the uncertainty in the power ratio of the reference signal. The derivation of this is shown in appendix C.3.1. The uncertainties of each of these terms are treated as correlated, to provide a worst-case-scenario estimate for the measurement uncertainty. Taking the definition for $\psi_{IntR\,[0,2\pi)}$ given in equations 3.1 and 3.2, the resulting uncertainty is simply given by,

$$\sigma_{\Delta\psi_{IntR\,[0,2\pi)}} = \sigma_{\Delta\psi_{IntR\,[0,\pi]}}. \tag{3.12}$$

3.4.2 Uncertainty in $\Delta\theta_{IntR}$

Taking equations 3.3 for $\Delta\theta_{IntR}$ and 3.4 for ψ_{off}, θ_{IntR} can be defined for both the slow and fast polarisations of the reference signal as follows,

$$\text{Slow: } \Delta\theta_{IntR} = \Delta\theta_{IntRS} - \psi_{off} \tag{3.13}$$

$$\text{Fast: } \Delta\theta_{IntR} = \Delta\theta_{IntRF}. \tag{3.14}$$

Therefore the uncertainty expression for the unwrapped phases is given by,

$$\text{Slow: } \sigma_{\Delta\theta_{IntR}} = \sigma_{\Delta\psi_{IntRS\,[0,2\pi)}} + \sigma_{\psi_{off}} \tag{3.15}$$

$$\text{Fast: } \sigma_{\Delta\theta_{IntR}} = \sigma_{\Delta\psi_{IntRF\,[0,2\pi)}} \tag{3.16}$$

where the uncertainty in ψ_{off} is the standard error of the mean phase offset and the subscripts S and F denote the phase for the slow and fast signals respectively. For each point in a dataset, the interferometer phase $\Delta\theta_{IntR}$ is chosen from either the slow or fast signal, depending on which signal has the lowest uncertainty $\sigma_{\Delta\theta_{IntR}}$ for that data point.

3.4.3 Uncertainty in $\Delta\psi_{IntQ}$

To convert the change in the interferometer phase experienced by the reference signal, $\Delta\theta_{IntR}$, into that experienced by the QKD signal, $\Delta\theta_{IntQ}$, the following equation from chapter 2 is used,

$$\Delta\theta_{IntQ} = \frac{\lambda_R}{\lambda_Q}\frac{n_{airQ}}{n_{airR}}\Delta\theta_{IntR} + \varepsilon_{Temp} + \varepsilon_{\lambda}. \tag{2.46, revisited}$$

λ_R and λ_Q are the reference and QKD signal wavelengths respectively, where the uncertainty in the wavelength fraction, λ_R/λ_Q, is given by,

$$\sigma_{\lambda_R/\lambda_Q} = \frac{\lambda_R}{\lambda_Q}\left(\frac{\sigma_{\lambda_R}}{\lambda_R} + \frac{\sigma_{\lambda_Q}}{\lambda_Q}\right). \tag{3.17}$$

In this work, the reference signal is provided by a Rio Orion laser module [73], which generates CW light with a peak wavelength of $\lambda_R = 1542.1 \pm 0.004$ nm. The QKD signal and probe signals are generated using the Pico Quant LDH-P-F-N-1550 laser [70] driven by the PDL 800-D laser diode driver [71], producing a pulsed signal with a peak wavelength of $\lambda_Q = 1549.512 \pm 0.004$ nm and a pulse full width half maximum of ~ 150 ps.

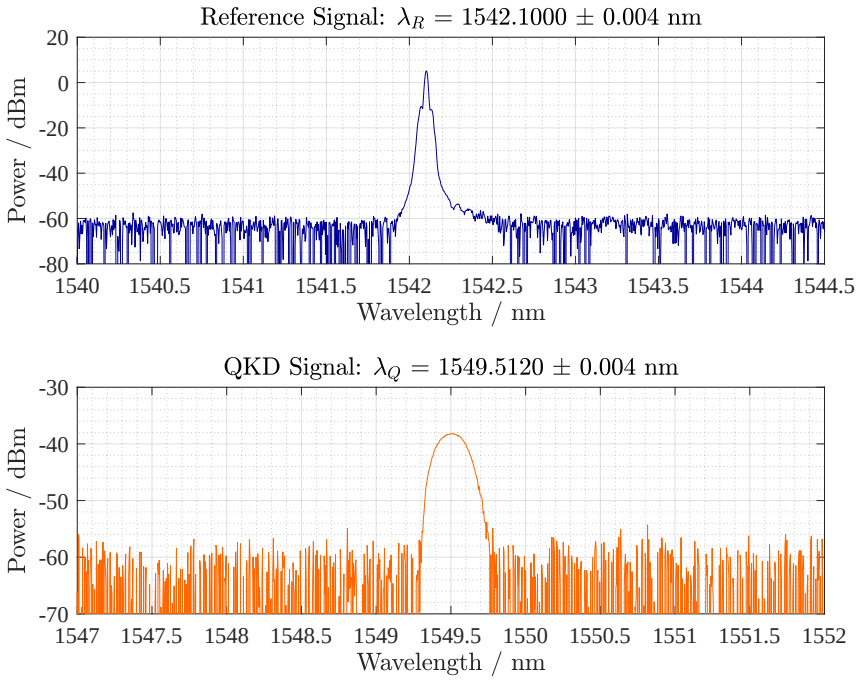


Figure 3.21: The optical spectra for the reference signal (Rio Orion laser module) and the QKD/probe signal used in this work (pulsed Pico Quant laser).

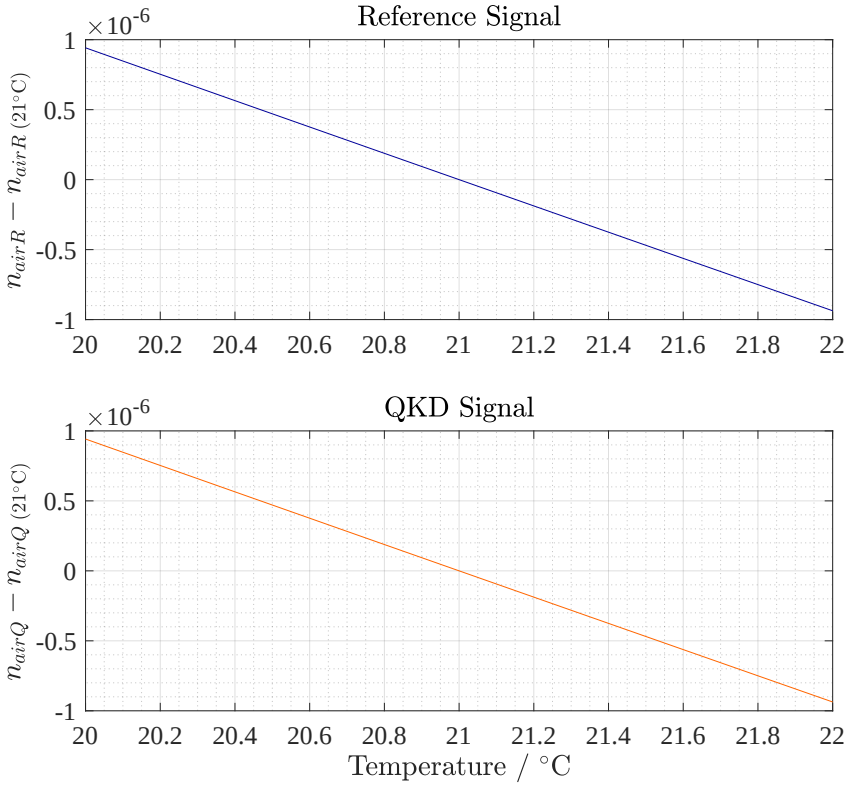


Figure 3.22: Change in the refractive index of air for the reference and the QKD signal for temperature changes around 21 °C.

The wavelength spectra for both of these laser signals are shown in figure 3.21, taken using the Yokogawa AQ6370D optical spectrum analyser. The uncertainty of the peak wavelengths results from the resolution on the analyser.

The uncertainty of the fraction of the refractive indices of air for the reference and the QKD signal, $\sigma_{n_{airQ}/n_{airR}}$, is given by,

$$\sigma_{n_{airQ}/n_{airR}} = \frac{n_{airQ}}{n_{airR}} \left(\frac{\sigma_{n_{airR}}}{n_{airR}} + \frac{\sigma_{n_{airQ}}}{n_{airQ}} \right). \tag{3.18}$$

From the Edlén equation [49–52], the change in the refractive index of air for a temperature range of 21 ± 1 °C is shown in figure 3.22. From these values the worst-case-scenario estimate for the uncertainty in the refractive index for both signals is $\sigma_{n_{airR}} = \sigma_{n_{airQ}} = 1 \times 10^{-6}$. These values can then be substituted into equation 3.18 to estimate the value of $\sigma_{n_{airQ}/n_{airR}}$. The total measurement uncertainty on the fully unwrapped interferometer phase for the QKD signal can be written as,

$$\sigma_{\Delta\theta_{IntQ}} = \theta_{IntQ} \left[\left(\frac{\sigma_{\Delta\theta_{IntR}}}{\Delta\theta_{IntR}} \right)^2 + \left(\frac{\sigma_{n_{airQ}/n_{airR}}}{n_{airQ}/n_{airR}} \right)^2 + \left(\frac{\sigma_{\lambda_R/\lambda_Q}}{\lambda_R/\lambda_Q} \right)^2 \right] + \varepsilon_{Temp} + \varepsilon_{\lambda} \tag{3.19}$$

where estimates for the values of the error terms ε_{Temp} and ε_{λ} are given in section 2.4. These equations are used to provide the estimates of the measurement uncertainties in the following chapters.

3.5 Measurement System Summary

The constructed measurement system consists of three main components,

- An AMZI
- Reference signal preparation and detection
- QKD signal detection/probe signal generation, for the characterisation of transmitters/receivers

The AMZI element has three levels of OPD control. The first is pulse selection, constructed out of optical fibre (if necessary) to select which pulses in the pulse train that are to be overlapped and interfered for the measurement. The second is pulse overlap tuning; adjustments made to the OPD in free space using an actuator controlled stage, to ensure the chosen pulses are well overlapped. The final is phase sweep and adjustment; a piezo element used to adjust the OPD in free space to perform sweeps of the interferometer phase and produce interference fringes. The system incorporates many optical and electronic controlled components to perform the functionality described in chapter 2. Software to control the measurement system and perform characterisation measurement has been developed, and procedures concerning both real-time and post phase analysis have been included.

Results of preliminary testing of the system have been presented, indicating its various functionality. The following chapters apply the measurement system in various experimental setups, utilising the phase and measurement uncertainty calculations detailed here. The phase calculations made for the data taken in the following chapters is post-processed; the real time functionality is not utilised.

Chapter 4

Assessment of Laser Sources and Pseudo QKD Signals

This chapter explores the application of the measurement system to assess the phase properties of optical sources. This demonstrates the functionality of the measurement system and provides a test of the transmitter-assessment formulation of the system and the measurement procedure. This chapter explores the application of the measurement system to assess the phase properties of laser sources, in particular the coherence of two continuous wave (CW) lasers and the incoherence between pulses from a pulsed laser source. In addition, the measurement system is used to assess the phase properties of pseudo QKD signals, where these signals are generated using a home-made experimental setup. These setups consist of a bright pulsed laser source, which is modified to produce a train of pulse pairs, where the phase difference between the pulses can be varied using a phase modulator. The resulting signal is a train of phase-modulated laser pulses, which can be bright or attenuated to the single-photon level to resemble a QKD signal, both of which can be applied to the measurement system.

4.1 Coherence Assessment of CW Sources

To assess a coherent CW laser source, the setup shown in figure 4.1 is used. The CW laser signal under test is passed through an isolator, a variable optical attenuator, polarisation control, a linear polariser and is then split by a 50:50 coupler, where half of the signal is sent to a monitoring power meter. The other half of the signal is sent into a circulator and then into the AMZI of the measurement system via the *IntQ* port. The circulator is implemented to reduce noise detected at D_{ML} resulting from the back-reflection of the reference signal prior to the 50:50 coupler; this is particularly critical for experiments in the single-photon regime. The AMZI is set to the tap-enabled state, with a 500 ps free-space optical path difference (OPD) and a quarter waveplate in the external arm, as shown in figures 3.2 and 3.6 in chapter 3. The CW laser signal under test is output from the AMZI at port *OutQ* and enters a wavelength division multiplexer and is then detected by a power meter. The reference signal is generated using the setup shown in figure 3.7 in chapter 3, and is sent into the AMZI via input port *InR*. The reference signal is then detected at the output *OutR* of the AMZI using a power meter. The reference signal and the CW laser signal under test propagate in opposite directions through the measurement system to reduce crosstalk. The experimental setup is used to assess two CW laser sources, the SFL1550P single frequency laser [76] and the T100S-HP tuneable frequency laser [77]

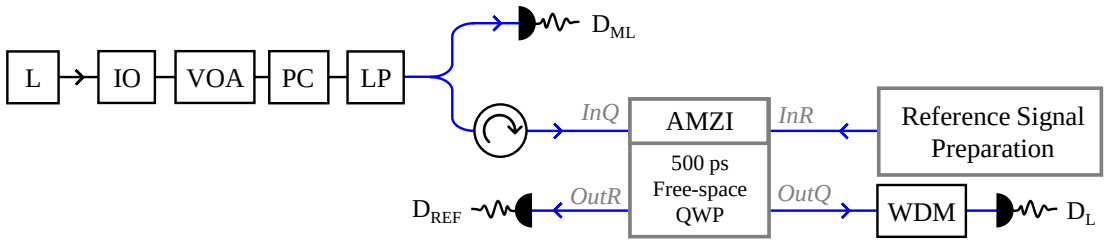


Figure 4.1: Schematic of the measurement system used to assess CW laser sources. The signal from the CW laser source (L) is passed through an isolator (IO), a variable optical attenuator (VOA), polarisation control (PC), a linear polariser (LP), into a 50:50 fibre coupler. One output is sent towards a monitoring power meter (D_{ML}) and the other output is sent through a circulator (circular arrow) and into the measurement system AMZI. This signal is output from *OutQ* and is sent through a wavelength division multiplexer (WDM) and detected using a power meter (D_L). The reference signal is prepared and input into the AMZI via *InR* and is detected at *OutR* by a power meter (D_{REF}). Black lines indicate single mode optical fibre and blue lines indicate single mode polarisation-maintaining optical fibre. Details of the AMZI setup can be found in figures 3.2 and 3.6 and details of the reference signal preparation can be found in figure 3.7 in chapter 3.

4.1.1 Single Frequency Laser Source (SFL1550P)

The single frequency laser (SFL) is the Thorlabs SFL1550P external cavity laser diode[76], operated via an external temperature controller and laser diode current driver. An optical spectrum analyser (Yokogawa AQ6370D) was used to measure the peak wavelength of the laser, $\lambda_{pk} = 1549.7$ nm, and the resulting spectrum is shown in figure 4.2. For this experiment, the optical power of the SFL signal used is 980 nW and the optical power of the reference signal slow and fast polarisations are 890 nW and 390 nW respectively.

To perform the phase measurement, the SFL source is input into the setup shown in figure 4.1 as the laser under test (L). The SFL signal is detected, along with the reference signal, and the voltage applied to the piezo element of the AMZI is repeatedly swept between 0 V and 70 V in incremental steps of 0.1 V. Details of the input reference signal are included in chapter 3, where the input polarisation of the reference signal is alternated between the slow and fast aligned states for each data point. The interference patterns from the two reference signal polarisations are recorded and the phase of each of these is calculated. The change in the interferometer phase experienced by the reference wavelength, $\Delta\theta_{IntR}$, is determined using the slow and fast reference signal, where the signal used is selected depending on which results in the lowest uncertainty $\sigma_{\theta_{IntR}}$. See sections 3.3.2 and 3.4.1 in chapter 3 for further details.

For one sweep of the piezo voltage between 0 V and 70 V, the phases of the reference signal, $\Delta\psi_{IntR\,[0,\pi]}$, $\Delta\psi_{IntR\,[0,2\pi)}$ and $\Delta\theta_{IntR}$, are shown in figure 4.3 for the slow and fast polarisations (top plot). The uncertainties in $\Delta\theta_{IntR}$, as defined in section 3.4, for each polarisation state are also shown (middle plot) and the final resulting data set for $\Delta\theta_{IntR}$ based on these uncertainties is indicated (bottom plot).

This final data set for $\Delta\theta_{IntR}$ is then converted into $\Delta\theta_{IntSFL}$, the change in the interferometer phase experienced by the SFL signal under test, using equation 2.46, with $\varepsilon_{Temp} = 0.1$ mrad and $\varepsilon_{\lambda} = 20$ mrad. For the same piezo sweep, the value of $\Delta\theta_{IntSFL}$ as well as the phases calculated from the SFL signal, $\Delta\psi_{SFL\,[0,\pi]}$, $\Delta\psi_{SFL\,[0,2\pi)}$ and $\Delta\theta_{SFL}$, are shown in figure 4.4 (top plot). The resulting uncertainty (calculations defined in section 3.4) for $\Delta\theta_{IntSFL}$ and $\Delta\theta_{SFL}$ are shown in the centre plot, where $\sigma_{\Delta\theta_{SLF}}$ increases

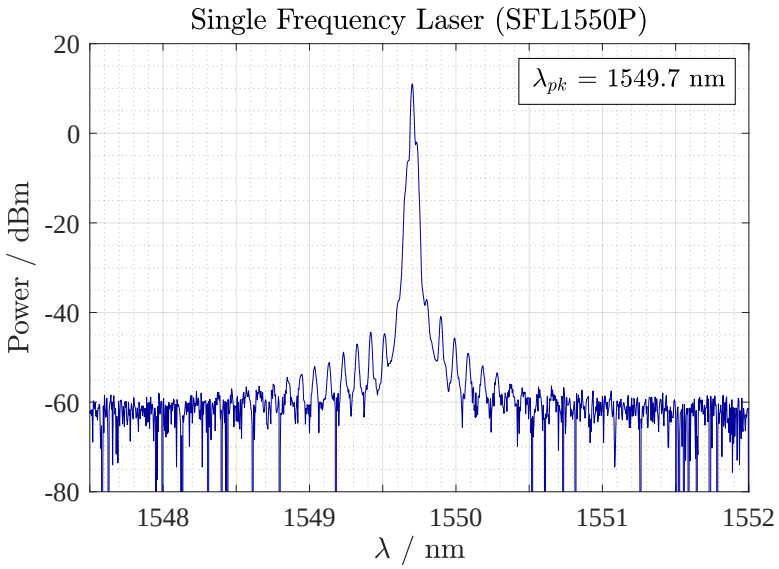


Figure 4.2: Measured optical spectrum of the single frequency SFL1550P laser.

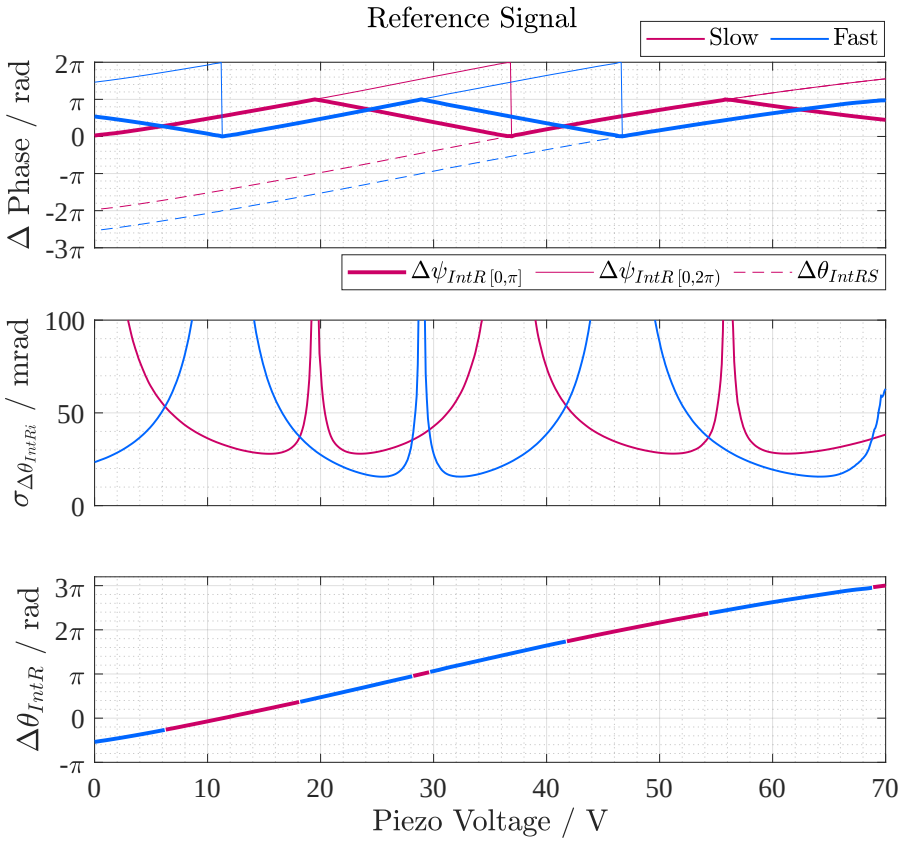


Figure 4.3: Results for the reference signal from one sweep of the piezo voltage. The top figure shows the phases calculated from the reference signal interference pattern for both the slow and fast polarisations. The centre plot shows the uncertainties calculated for the unwrapped interferometer phase, $\sigma_{\Delta\theta_{IntRi}}$ for $i = S, F$, for both polarisations. The bottom plot shows the final compounded dataset for $\Delta\theta_{IntR}$, which uses a mixture of the fast and slow polarisation signals as indicated, dependent on which results in the lowest final uncertainty.

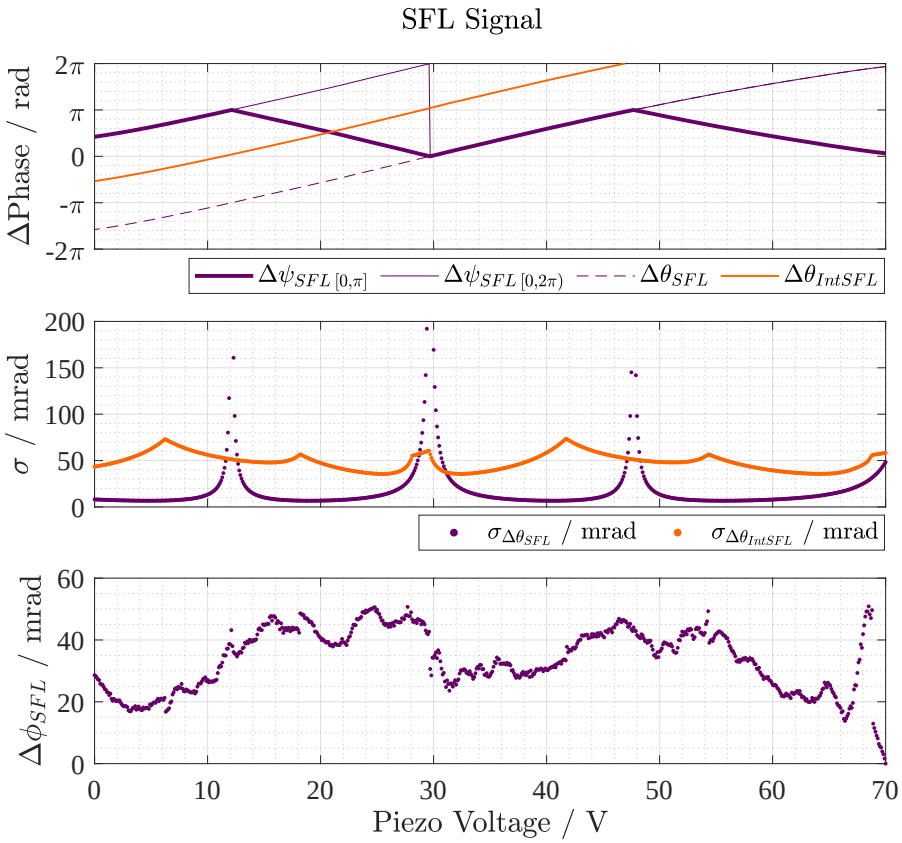


Figure 4.4: Results from the SFL signal from one sweep of the piezo voltage. The top figure shows the phases calculated from the SFL signal interference pattern and the change in the interferometer phase for the SFL signal calculated from $\Delta\theta_{IntR}$ in figure 4.3. The centre plot shows the uncertainties for $\Delta\theta_{SFL}$ and $\Delta\theta_{IntSFL}$. The bottom plot shows the measured change in phase of the input CW SFL signal.

significantly around the values of $\Delta\psi_{SFL\,[0,\pi]} = 0, \pi$, which is equivalent to the peaks and troughs of the SFL interference pattern. Comparatively, the uncertainty in the interferometer phase, $\sigma_{\Delta\theta_{IntSFL}}$, does not exceed 80 mrad, as this is calculated from the reference signal interferometer phase $\Delta\theta_{IntR}$. This directly demonstrates the benefit of using two polarisation states of the reference signal that are phase offset from one another, such that the interferometer phase can be calculated from both signals avoiding these asymptotic-style uncertainty values. Finally, the interferometer phase $\Delta\theta_{IntSFL}$ and the SFL measured phase $\Delta\theta_{SFL}$ are combined to calculate the original phase difference of the SFL signal $\Delta\phi_{SFL}$. As the SFL is a CW laser, the light is expected to be coherent over the short AMZI OPD of 500 ps. Therefore, the measured value of $\Delta\phi_{SFL}$ should not change over the sweeps of the piezo voltage. From this single piezo sweep, the final plot in figure 4.4 shows a maximum variation in the SFL signal phase of $\Delta\phi_{SFL} < 60$ mrad, $< \lambda_{SFL}/100$.

Repeated sweeps of the piezo voltage are performed and the resulting values of $\Delta\phi_{SLF}$ are shown in figure 4.5[1]. Sweeps are performed just after the laser is switched on and then again ~ 22 hours later. Both the upper and lower plots show the data points, where

[1]Details of the analysis code used to calculate all of the phases for this experiment and the subsequent experiments detailed in this work is given in appendix D.1. This includes important details on referencing the change in the interferometer phase between piezo sweeps.

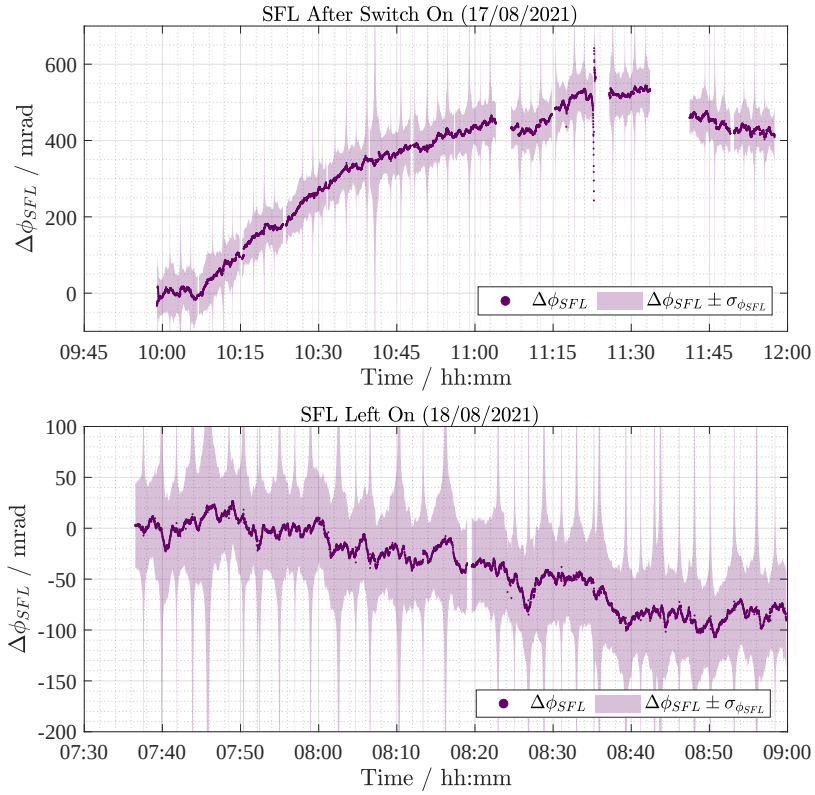


Figure 4.5: Change in the SFL phase for many sweeps of the piezo voltage. The purple dots are the data points and the light purple shaded region indicates the measurement uncertainty on the stated phase value. The upper plot shows the phase change soon after the laser was switched on. The lower plot shows the phase change after the SFL was left on for approximately 22 hours. Note that the range of the y-axis of the upper plot is 700 mrad, where as the range of the y-axis on the lower plot is 300 mrad.

the shaded regions represent the measurement uncertainty on the phase value $\sigma_{\phi_{SFL}}$. The sharply increasing and decreasing areas in the uncertainty region result from the uncertainty of the SFL phase, $\sigma_{\Delta\theta_{SFL}}$, as shown in the middle plot in figure 4.4. These asymptotic-style uncertainties cannot be avoided as they result from the inherent properties of phase measurement and the signal under test. Namely, attempting to measure the phase of the signal at the peaks and troughs of the interference pattern will result in a high uncertainty, given the sinusoidal nature of the power ratio to phase relationship. The change in the measured phase of the SFL signal drifts significantly after the laser is switched on. After the 22-hour stabilisation period the recorded drift in the SFL phase has noticeably decreased, but a drift of -1.1 mrad per minute remains.

4.1.2 Tuneable Frequency Laser Source (T100S-HP)

The tuneable frequency laser (TFL) by EXFO [77], T100S-HP, is a high power continuously tuneable laser. The TFL was set to output a wavelength of 1550 nm and an optical spectrum analyser was used to measure the peak wavelength signal, $\lambda_{pk} = 1549.996$ nm, where the resulting optical spectrum is shown in figure 4.6. For this experiment, the optical power of the TFL signal used is 990 nW and the optical power of the reference signal slow and fast polarisations are 1.02 µW and 300 nW respectively.

The same measurement procedure as described previously for the SFL signal is carried

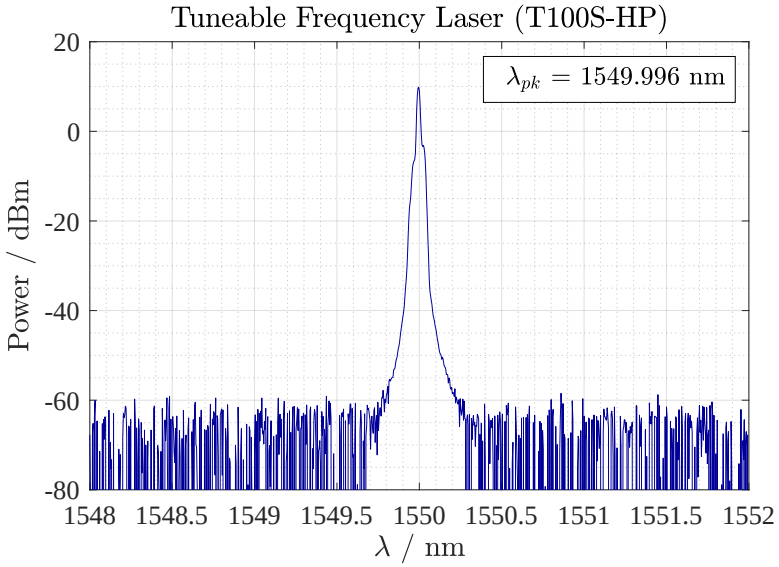


Figure 4.6: Measured optical spectrum of the TFL signal.

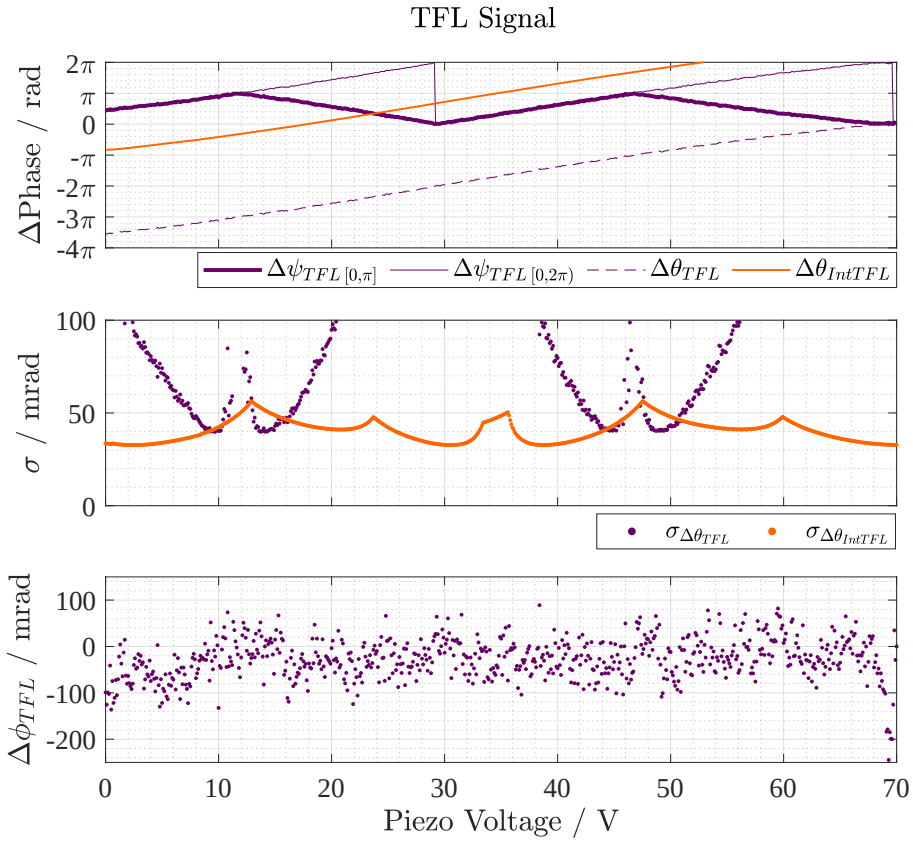


Figure 4.7: Results from the TFL signal from one sweep of the piezo voltage. The top figure shows the phases calculated from the TFL signal interference pattern ($\Delta\psi_{TFL\,[0,\pi]}$, $\Delta\psi_{TFL\,[0,2\pi)}$, $\Delta\theta_{TFL}$) and the change in the interferometer phase for the TFL signal ($\Delta\theta_{IntTFL}$) calculated from $\Delta\theta_{IntR}$. The centre plot shows the uncertainties for $\Delta\theta_{TFL}$ and $\Delta\theta_{IntTFL}$. The bottom plot shows the change in phase of the TFL signal over the sweep.

out for the TFL signal. The TFL source is input into the setup shown in figure 4.1 as the laser under test (L). The TFL signal and the reference signal (both polarisations) are recorded as the voltage applied to the piezo element in the AMZI is repeatedly swept between 0 V to 70 V in incremental steps of 0.1 V. The reference signal is used to calculate the interferometer phase $\Delta\theta_{IntR}$, which in turn is used to calculate the interferometer phase experienced by the TFL signal wavelength, $\Delta\theta_{IntTFL}$. Once again, $\varepsilon_{Temp} = 0.1$ mrad and $\varepsilon_{\lambda} = 20$ mrad. For a single sweep of the piezo voltage between 0 V and 70 V, the value of $\Delta\theta_{IntTFL}$ as well as the phases calculated from the TFL signal, $\Delta\psi_{TFL\,[0,\pi]}$, $\Delta\psi_{TFL\,[0,2\pi)}$ and $\Delta\theta_{TFL}$, are shown in figure 4.7 (top plot). The resulting uncertainty for $\Delta\theta_{IntTFL}$ and $\Delta\theta_{TFL}$ are shown in the centre plot, where once again the uncertainty in the TFL phase $\sigma_{\Delta\theta_{TFL}}$ increases significantly at $\Delta\psi_{TFL\,[0,\pi]} = 0, \pi$; the peaks and troughs of the TFL interference pattern. The interferometer phase $\Delta\theta_{IntTFL}$ and the TFL measured phase $\Delta\theta_{TFL}$ are combined to calculate the original phase difference of the TFL signal $\Delta\phi_{TFL}$, shown in the bottom plot of figure 4.1. The resulting plot of $\Delta\phi_{TFL}$ shows little variation in the phase over the course of the piezo sweep, but a much higher phase noise level of $\pm$100 mrad compared to the SFL laser.

Repeated sweeps of the piezo voltage are performed and the resulting values of $\Delta\phi_{TLF}$ are shown in figure 4.8. Sweeps are performed just after the laser was switched on and then again $\sim$ 18 hours later. Both plots show the data points and a shaded region representing the measurement uncertainty on the phase value, $\sigma_{\phi_{SFL}}$, where the sharply increasing and decreasing areas in the uncertainty region result from the asymptotic-style uncertainties in the TFL signal discussed previously ($\sigma_{\Delta\theta_{TFL}}$). After 18 hours, the drift and noise of the TFL phase are similar in both datasets. This is most likely due to the phase noise masking any noticeable phase drift in the TFL signal.

The resulting increased noise in the phase values of the TFL CW signal, compared to the SFL signal, is not inherently strange as any change to the peak wavelength or varying presence of other wavelengths in the signal will result in different measured phase values. However, from the spectra shown for the SFL and the TFL in figures 4.2 and 4.6 respectively, the two signals have a similar linewidth, with a full width half maximum of $\sim$ 17 pm. This would suggest that other wavelengths within the TFL signal are not present, and therefore are not the source of the phase noise. An additional contribution to the noise may be due to the running mode of the laser. For the experiment above the TFL was operated in constant power mode, where the drive current is varied to maintain the output power of the laser. A shorter experiment was performed operating the TFL in constant current mode, performing five sweeps of the piezo voltage. The resulting phase of the signal is shown in the top plot of figure 4.9 soon after the laser was switched on. The phase drifts substantially at the start of the measurement, and then again towards the end of the measurement. However, the phase noise is significantly less, highlighted by the bottom plot of figure 4.9, which shows the change in phase values from the third sweep of the piezo element (initialised to the phase at the start of the sweep). The phase noise is approximately $\pm$25 mrad, which is better than that for the TFL in constant power mode.

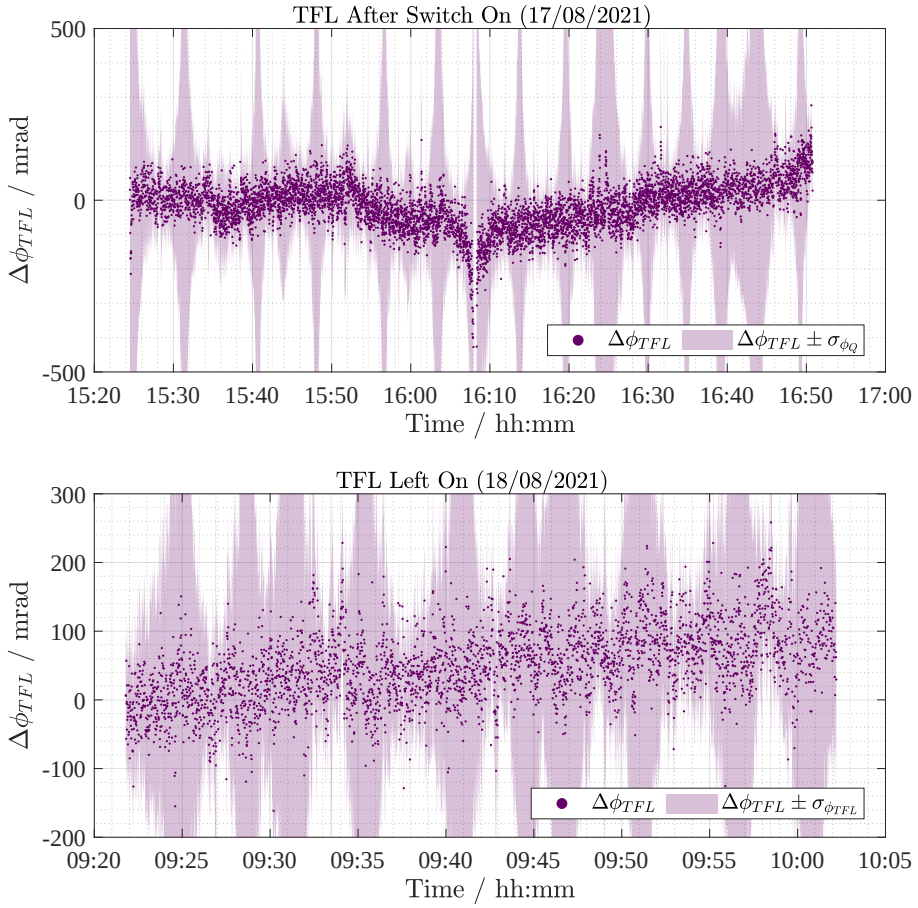


Figure 4.8: Change in the TFL phase for many sweeps of the piezo voltage when operated in constant power mode. The purple dots are the data points and the light purple shaded region indicates the measurement uncertainty on the stated phase value. The upper plot shows the phase change soon after the laser was switched on. The lower plot shows the phase change after the TFL was left on for approximately 18 hours. Note that the top plot measurement duration is 85 minutes, where as the measurement duration of the bottom plot is 40 minutes.

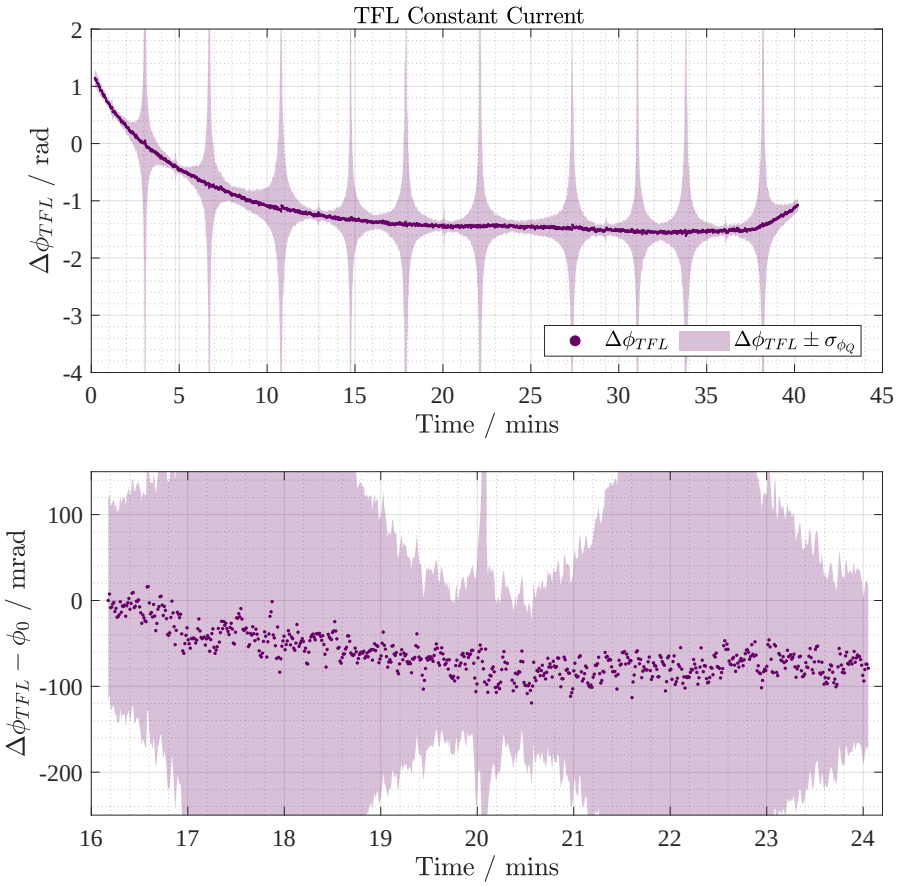


Figure 4.9: Resulting phase of the TFL signal when the laser is operated in the constant current mode. The top plot shows the resulting phase for all five sweeps of the piezo voltage. The bottom plot shows the resulting phase for just the third sweep, initialised according the starting phase value of the sweep.

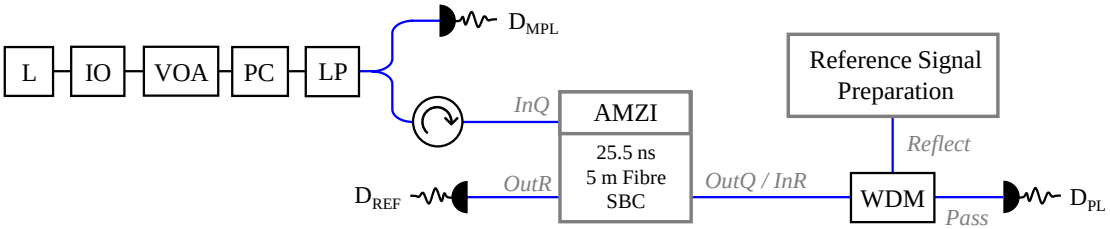


Figure 4.10: Schematic of the setup used to assess the PicoQuant PL signal, consisting of the PL (L), an isolator (IO), a variable optical attenuator (VOA), polarisation control (PC), linear polariser (LP), 50:50 fibre coupler, a circulator (circular arrow), AMZI, wavelength division multiplexer (WDM) and detectors (D_{MPL}, D_{PL}, D_{REF}). Single mode fibre is represented by black lines and polarisation-maintaining single mode fibre is represented by blue lines. The reference signal is sent into the AMZI via the multiplexer[2].

4.2 Coherence Assessment of a Pulsed Source

CW laser light is coherent, such that it will exhibit the effects of interference within the coherence length of the laser. However, for a pulsed laser, different methods of pulses generation will result in either coherent or incoherent laser pulses. Incoherence specifically arises when the laser cavity is depleted of all photons between emission, such that each laser pulse is generated via spontaneous emission, where the resulting phase of the light is randomised [37]. The following is an assessment of the coherence of a pulsed laser diode.

4.2.1 PicoQuant Pulsed Laser

The pulsed laser (PL) signal used is generated via a PicoQuant LDH-P-F-N-1550 laser diode [70] driven by the PicoQuant PDL 800-D laser driver [71]. This laser is referred to in section 3.4.3, where the optical spectrum for this laser is shown in the QKD Signal plot in figure 3.21. To assess the coherence and potentially measure the phase of the PL signal, the pulses are sent into the measurement system, where the AMZI asymmetry is equivalent to the temporal separation between the pulses. The setup used to achieve this is shown in figure 4.10. The pulsed laser signal is sent through an isolator, a variable optical attenuator, polarisation control a linear polariser and then a 50:50 coupler. Half of the signal is monitored by the detector D_{MPL} and the other half of the signal is sent into a circulator and into the AMZI. The AMZI has an OPD equivalent to a delay of 25.5 ns, which is achieved by enabling the tap and using a 5 m fibre extension to the external arm, see figures 3.2 and 3.5 in chapter 3 for further details. The pulsed signal exits the AMZI via the *OutQ* port and passes through a WDM and is detected by D_{PL}. The CW reference signal is prepared, see figure 3.7, and is sent into the AMZI via the reflect port of the wavelength division multiplexer[2] and is detected at port *OutR* at detector D_{REF}. The input power of the PL signal is 110 nW and the input power of the slow and fast polarisations of the reference signal are 930 nW and 400 nW respectively.

The OPD of the AMZI is set to overlap the pulses of the PL signal, where the temporal separation between pulses is 25.5 ns. A trace of the pulse train outputted from the PL and sent through the measurement system is detected using the Thorlabs DXM30AF fast

[2]The input of the reference signal into the AMZI via the multiplexer here is different to the previous setup of the phase measurement experiment, where previously the reference signal was sent in via a separate port. This new formulation of the setup was used to assess whether improved separation of the reference signal and the signal under test could be achieved. The new setup did not change the separation of the two signals, and is operationally identical to the previous setups shown.

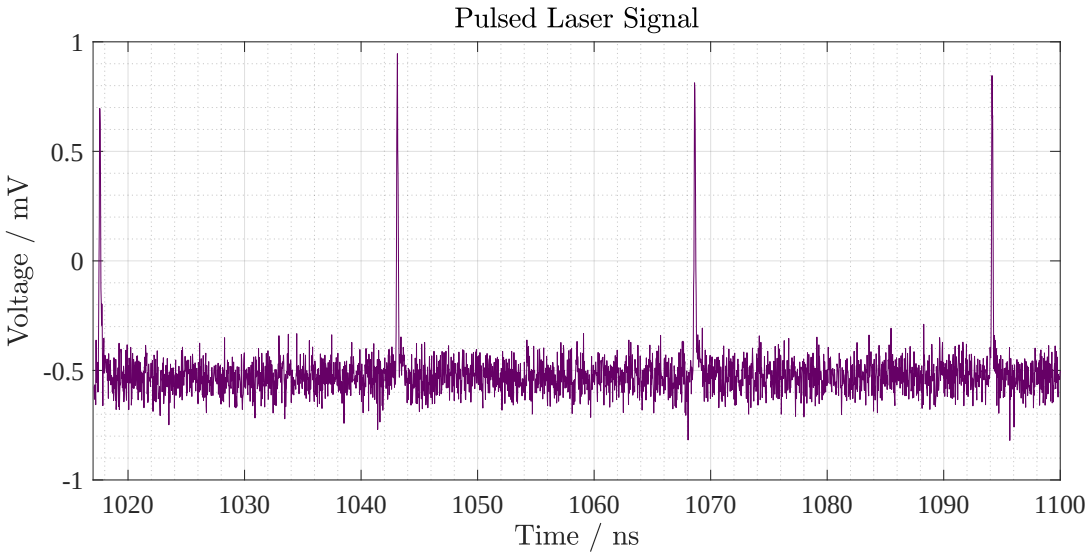


Figure 4.11: Measured trace of the pulsed laser signal, showing multiple pulses with a temporal separation of 25.5 ns.

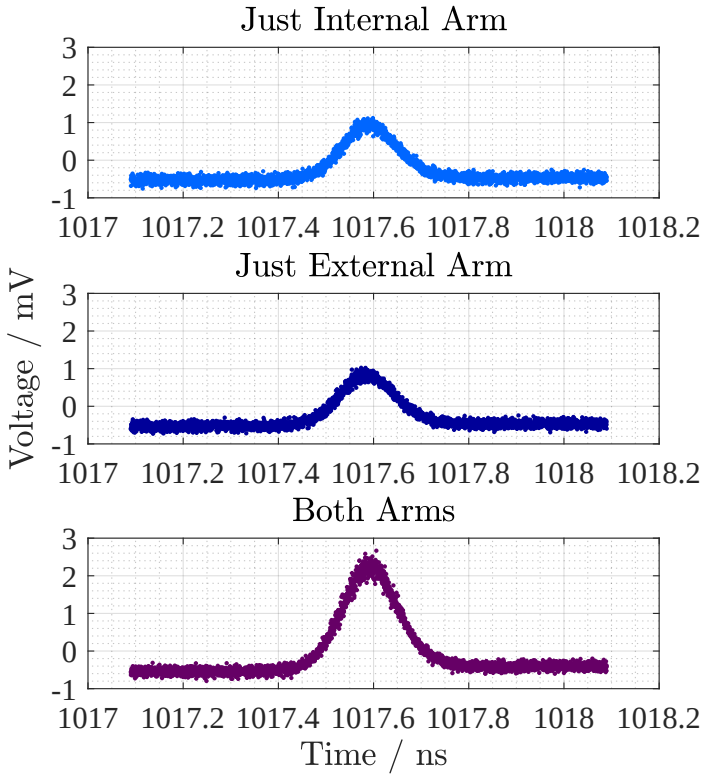


Figure 4.12: Traces of the PL signal, where the pulses propagate through just the internal arm of the AMZI (top), just the external arm of the AMZI (middle) and through both arms of the AMZI (bottom).

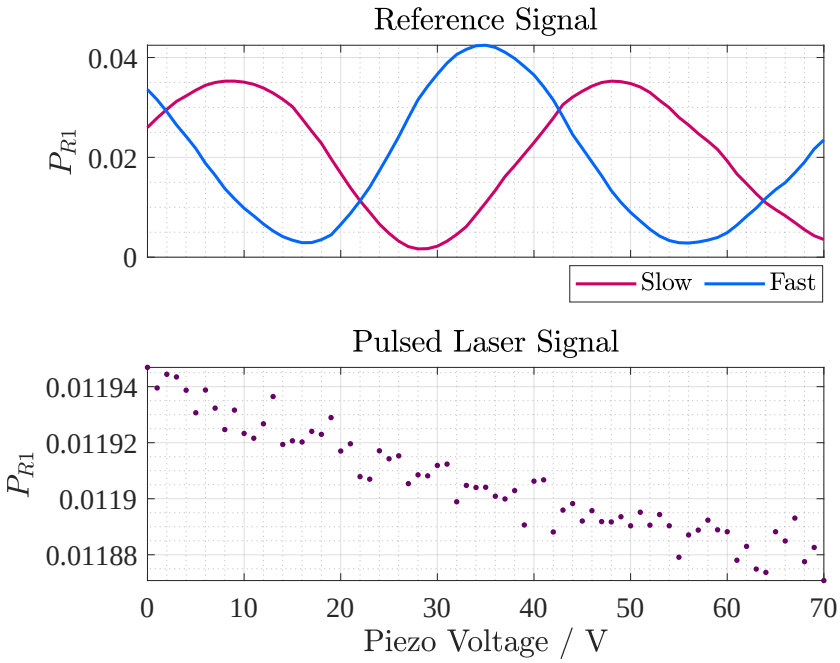


Figure 4.13: Plot of the power ratio P_{R1} for the reference signal and the pulsed laser signal for one sweep of the piezo voltage between 0 V and 70 V.

photodetector [72] and is shown in figure 4.11. Separate traces are taken of one pulse in the train for the following three cases:

- When the signal passes through just the internal arm of the AMZI (external arm blocked)
- When the signal passes through just the external arm of the AMZI (internal arm blocked)
- When the signal passes through both arms of the AMZI

The traces for each of these cases are shown in figure 4.12, where it can be seen that the pulses of the pulse train are temporally overlapped by the AMZI.

To assess the coherence of the PL, the voltage applied to the piezo element is swept between 0 V and 70 V in incremental steps of 1 V. The sweeps of the piezo voltage are performed for the three states of the AMZI detailed above (just internal, just external and both arms). For each of these cases, the voltage of the piezo element is swept eight times in succession. When the signals are allowed to pass through both arms of the AMZI, the detected CW reference signal exhibits an interference pattern, as anticipated, but the PL signal shows no interference effect. This is shown in plots of the power ratios for one sweep of the piezo displayed in figure 4.13. Although there is no interference pattern, the power ratio of the PL signal does decrease with the increasing piezo voltage by -0.67%. This is due to the variation in the transmittance of the external arm with the changing piezo voltage, as explored in chapter 3. To demonstrate this, the power ratio for all eight sweeps of the piezo voltage for the three states of the AMZI are shown in figure 4.14. For all eight sweeps, the internal arm shows no change in the power ratio, indicating that there is no change to the transmittance of the internal arm with the piezo voltage. However, there is clear negative correlation between the transmittance of the external arm and the piezo voltage. Adding these two signals together and comparing this to the voltage sweeps performed when the signal is sent through both arms, as shown in the bottom plot of

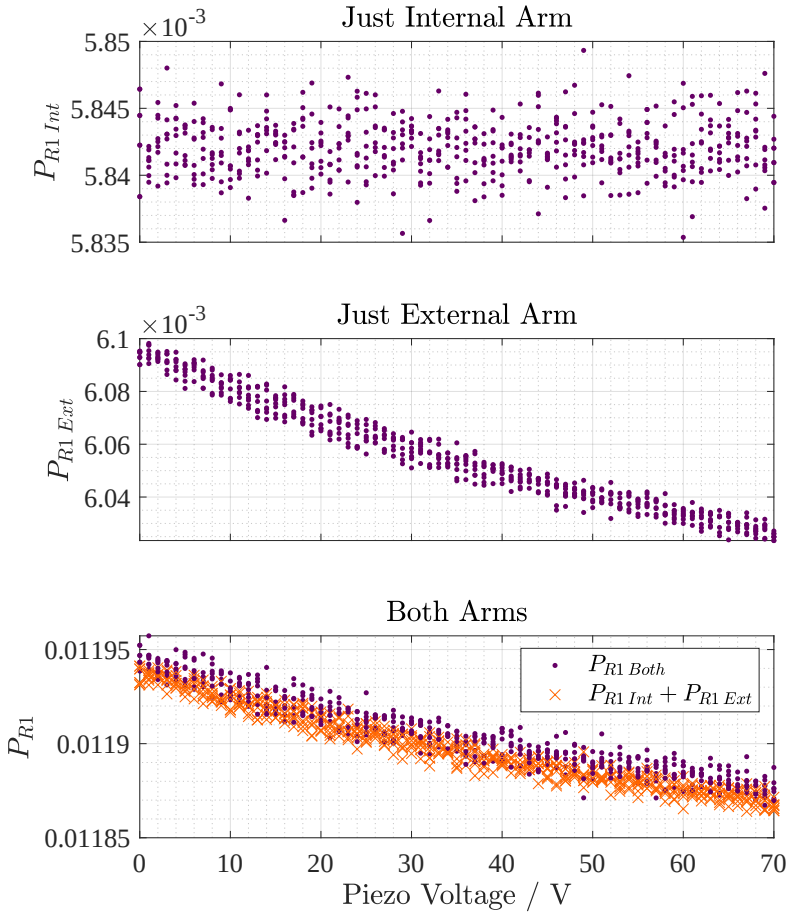


Figure 4.14: Power ratio P_{R1} of the pulsed signal for eight sweeps of the piezo voltage between 0 V and 70 V, when propagating through just the internal arm (top), just the external arm (middle) and both of the AMZI arms (bottom). The bottom plot also shows the sum of the power ratios from the top and middle plot, comparing this sum with the measured power ratio from propagation through both arms.

figure 4.14, it is clear that this change in the power ratio with the piezo voltage is directly due to the transmittance of the external arm and is not related to interference.

When the signal is allowed to propagate through both arms of the AMZI, the power ratio datasets for all eight sweeps can be corrected for the change in the transmittance of the external arm. To do this, the recorded power ratio datasets shown in figure 4.14 are referred to as, $P_{R1\,Int}$, when the signal propagates through the internal arm, $P_{R1\,Ext}$ when the signal propagates through the external arm and $P_{R1\,Both}$, when the signal propagates through both arms. To correct $P_{R1\,Both}$, firstly the mean power ratio of the internal arm is subtracted,

$$P_{R1(No\,Int)} = P_{R1\,Both} - \mu_{P_{R1\,Int}}. \tag{4.1}$$

Next, the change in the power ratio of the external arm compared to the mean is calculated,

$$\Delta P_{R1\,Ext} = P_{R1\,Ext} - \mu_{P_{R1\,Ext}} \tag{4.2}$$

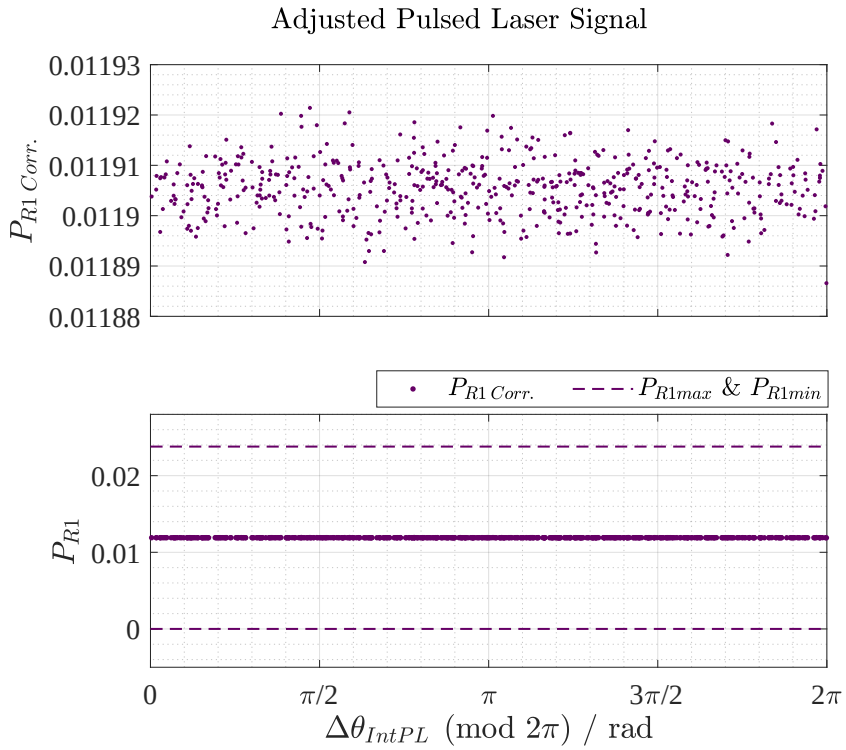


Figure 4.15: The corrected power ratio for the eight sweeps of the piezo voltage where the signal is allowed to propagate through both arms of the AMZI. $P_{R1\,Corr.}$ is plotted (top) against the phase change in the interferometer experienced by the pulsed laser wavelength, calculated using the CW reference signal. The bottom plot shows the same $P_{R1\,Corr.}$ data set also plotted alongside the predicted minimum and maximum of the interference pattern if the pulsed signal had been coherent.

and is applied to the value of $P_{R1(No\,Int)}$ as follows,

$$P_{R1(Ext\,adj.)} = P_{R1(No\,Int)} - \frac{\mu_{P_{R1(No\,Int)}} \Delta P_{R1\,Ext}}{\mu_{P_{R1\,Ext}}} \tag{4.3}$$

removing the variation of the transmittance of the external arm. Finally, the corrected power ratio for both arms is given by,

$$P_{R1\,Corr.} = P_{R1(Ext\,adj.)} + \mu_{P_{R1\,Int}}. \tag{4.4}$$

This corrected value of the power ratio for both arms is shown in the top plot of figure 4.15. The corrected power ratio is plotted against the interferometer phase change $\Delta\theta_{IntPL}$ (mod 2π) experienced by the PL signal, calculated from the CW reference signal. The resulting power ratio shows a flat line across the interferometer phase, indicating that the incoming pulses are incoherent with one another. To demonstrate this further, the internal and external data sets are used to estimate what the maximum and minimum of the interference pattern would be for the pulsed signal, and the resulting limits are also plotted alongside $P_{R1\,Corr.}$ in the bottom plot of figure 4.15. The method of estimating this minimum and maximum is shown in appendix D.2.

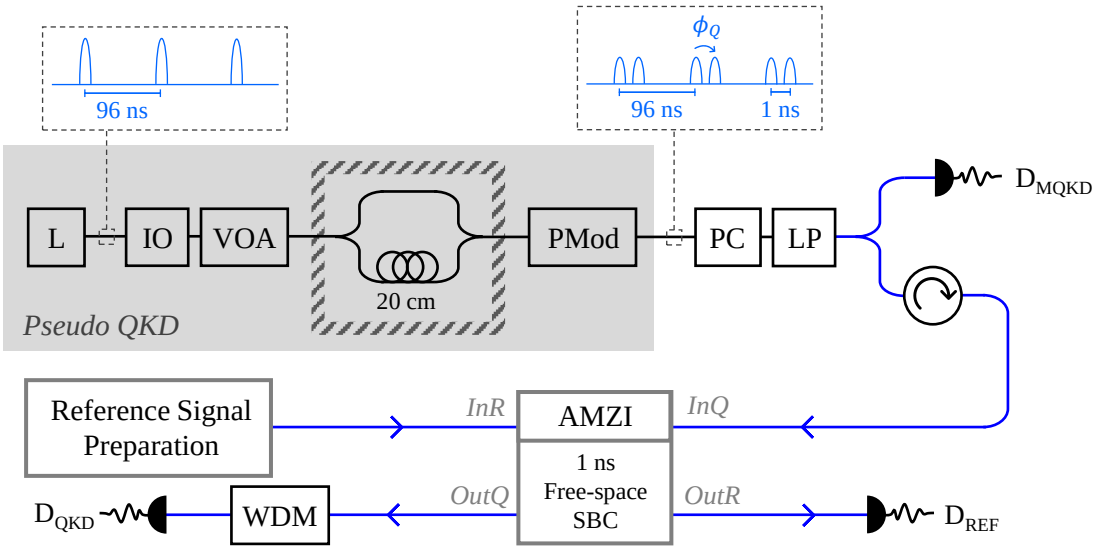


Figure 4.16: Schematic of the experimental setup used to generate the pseudo QKD signal and measure the phase of this signal. The setup consists of a pulsed laser (L), isolator (IO), variable optical attenuator (VOA), passively insulated fibre AMZI (grey dashed box), phase modulator (PMod), polarisation controls (PC), linear polariser (LP), circulator (circle with arrow), measurement system AMZI, wavelength division multiplexer (WDM), photodiode (D_{REF}) and power meters (D_{MQKD} and D_{QKD}). Black lines indicate single mode fibre and blue line indicate polarisation-maintaining single mode fibre. The grey shaded box indicates the devices used to generate the pseudo QKD signal and the dashed boxes at the top of the diagram indicate the state of the pseudo QKD signal at different points in the system. Details of the reference signal preparation can be found in chapter 3, figure 3.7.

4.3 Assessment of Pseudo QKD Signals

To operate the measurement system as it would be used in a QKD phase characterisation measurement, a pseudo QKD signal, generated using a home-made experimental setup of lab components, is assessed. The pseudo QKD signal can be generated using the aforementioned pulsed laser, a fibre AMZI and phase modulating components. This section explores an initial trial experiment using a pseudo QKD signal and a more developed experiment with a bright and dim pseudo QKD signal.

4.3.1 Trial Experiment

The trial experiment involves generating a pseudo QKD signal, a train of pulse pairs where the phase difference between the pulses in each pair is varied, and measuring the phase between the pulses using the measurement system. The experimental setup is shown in figure 4.16. The pseudo QKD signal, grey shaded area, consists of the PicoQuant pulsed laser [71], which generates a train of pulses with a temporal separation of ~ 96 ns. Each pulse has a full width half maximum of ~ 115 ps and the signal has an optical power of 240 nW at a wavelength of 1549.512 nm, see the optical spectrum in the lower plot of figure 3.21 in chapter 3. The pulsed signal is passed into an isolator, a variable optical attenuator and then a passively insulated optical fibre AMZI constructed out of two fibre couplers and a fibre patch cord. The fibre AMZI has an OPD of 20 cm, equivalent to a temporal delay of ~ 1 ns, where the passive insulation is the same as that described in section 2.3.2

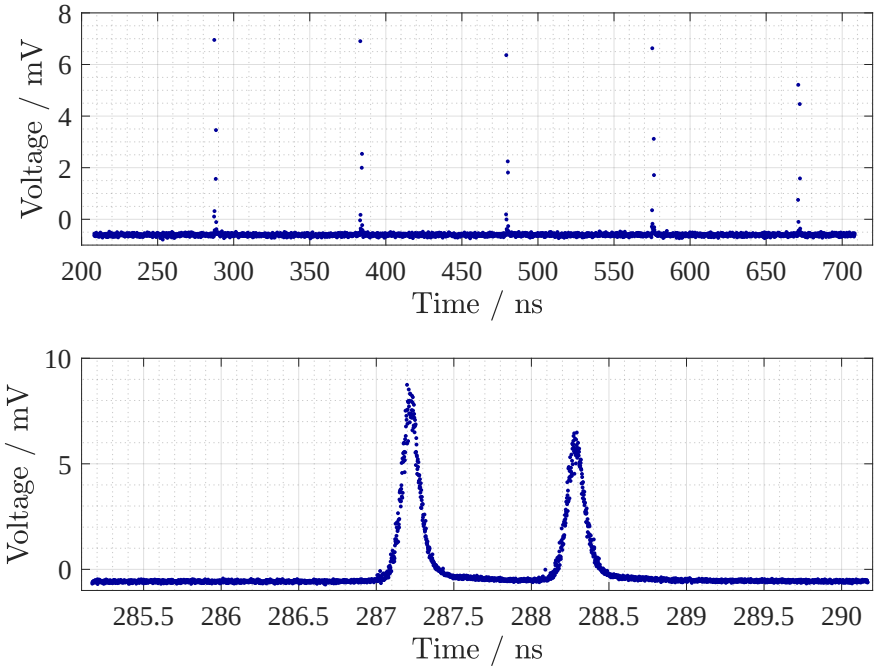


Figure 4.17: Pulses of the Pseudo QKD Signal before they enter the AMZI system. The top plot shows the pulse train of multiple pulse pairs. The bottom plot shows a single pair of pulses generated from one pulse of the laser source after passing through the fibre AMZI.

and aims to reduce changes to the OPD over the measurement time. By propagating the pulsed signal through the fibre AMZI, each pulse is converted into a coherent pair of pulses that are separated by 1 ns. The pulses are then sent into a phase modulator that is used to apply a phase shift of ϕ_Q to one of the pulses in each pair. The resulting output is a train of pulse pairs, where the phase difference between the pulses corresponding to a single pair is ϕ_Q. Traces of the output pseudo QKD signal are shown in figure 4.17, where the upper plot shows the train of pulse pairs and the lower plot shows a single pulse pair.

The outputted pseudo QKD signal is then sent into polarisation controls, a linear polariser and is then split by a 50:50 fibre coupler, where half of the signal is sent towards a monitoring power meter, D_{MQKD}, and the other half is sent through a circulator and into the measurement system AMZI via port *InQ*. The signal exits the AMZI and is filtered via a wavelength division multiplexer and is detected by another power meter, D_{QKD}. The AMZI is set to the tap-enabled state with a free-space extension resulting in an OPD of $\sim$ 1 ns, which also contains the Soleil-Babinet compensator. Therefore the pulses in the pulse pairs of the pseudo QKD signal are overlapped and interfered by the measurement system AMZI. The two polarisation states of the reference signal are prepared and sent into the measurement system AMZI and are detected at the AMZI output using a photodiode, D_{REF}. The CW reference signal is generated by the Rio Orion laser [73], with a peak wavelength of 1542.1 nm, see the optical spectrum in the upper plot of figure 3.21 in chapter 3. The input power of the slow and fast signals are 1.1 µW and 600 nW respectively. Details on the preparation of the reference signal are given in chapter 3 in figure 3.7.

To create the pseudo QKD signal, a voltage is applied to the phase modulator (Thorlabs LN53S-FC) to generate the phase shift ϕ_Q. The voltage signal is a voltage pulse with a full width half maximum of 3.2 ns, generated using a Tektronix AWG70001A arbitrary

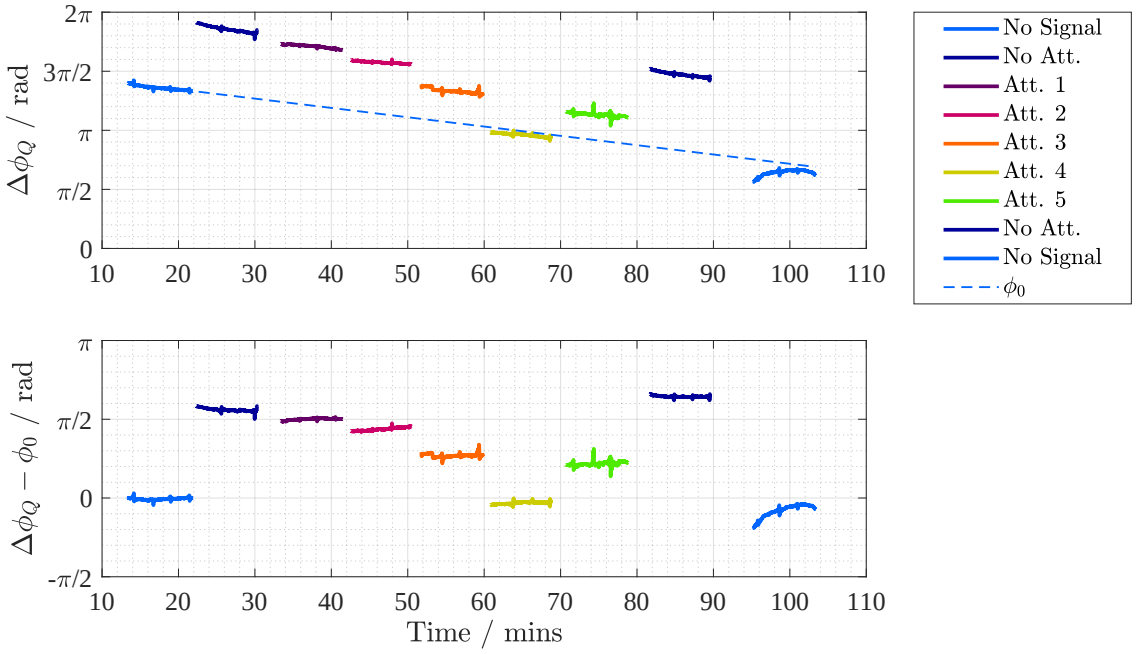


Figure 4.18: Calculated phases of the QKD signal, where each line corresponds to a piezo sweep for a different attenuator setting. The sweep lines from left to right correspond to each entry ordered in the legend list. In the top plot a first order polynomial is fit to the first data set corresponding to no applied modulator signal using a least squares fit. The resulting function, ϕ_0, is extrapolated out over the measurement duration. The difference between the calculated QKD phase $\Delta\phi_Q$ and ϕ_0 is then plotted for each sweep in the bottom graph.

waveform generator [78] and an amplifier. The waveform generator is also used to trigger the pulse generation of the laser, so that the voltage signal can be applied to the phase modulator in time with the arrival of one of the pulses in the pulse pair. The time difference between the trigger signal supplied to the laser and the voltage signal supplied to the phase modulator is adjusted, whilst monitoring the power ratio of the pulsed signal detected at D_{MQKD} and D_{QKD}. The delay between the two signals is considered optimised when the maximum change in the power ratio is observed; where the change in the power ratio is determined by switching the voltage signal supplied to the phase modulator on and off.

To vary the peak voltage applied to the modulator, in-line fixed attenuators (mini-circuits) are connected to the electrical link, reducing the signal strength. For each attenuator added, a phase sweep of the piezo voltage is performed, varying between 0 V and 65 V with an incremental step of 0.1 V. The reference signal is used to calculate the change in the interferometer phase as experienced by the pseudo QKD signal, $\Delta\theta_{IntQ}$. This in turn is used to calculate the phase difference between the incoming pulse pairs $\Delta\phi_Q$. The details of the attenuator combinations are given in table 4.1 and the resulting calculated values of $\Delta\phi_Q$ are plotted in the top graph of figure 4.18. The OPD of the passively insulated fibre AMZI (used to generate the pulse pairs) is not constant over the course of the measurement due to thermal fluctuations in the laboratory. This is evident from the values of $\Delta\phi_Q$ corresponding to the first voltage sweep data set, when no signal is applied to the phase modulator, shown in the top plot of figure 4.18. The value of $\Delta\phi_Q$ drifts over the measurement time of ~ 8 minutes. To account for this, a straight line ϕ_0 is fit to this initial dataset using the least squares method and the function is extrapolated over the entire measurement duration. The difference between the calculated phases $\Delta\phi_Q$ and ϕ_0

Attenuator Setup	**Number of Attenuators**	**Peak Voltage / V**	**Mean $\Delta\phi_Q - \phi_0$ / rad**
No Signal	0	0	0, -0.23
No Att.	0	3.33	1.78, 2.04
Att. 1	1	2.94	1.59
Att. 2	2	2.71	1.39
Att. 3	3	2.36	0.87
Att. 4	4	2.11	-0.08
Att. 5	1	1.07	0.702

Table 4.1: Details of the attenuator combinations applied to vary the voltage signal supplied to the phase modulator for the generation of the pseudo QKD signal. The number of attenuators and the resulting peak voltage are detailed, as well as the resulting change in the calculated QKD phase $\Delta\phi_Q - \phi_0$. Due to multiple attenuators being used, the voltage pulse may be offset to the incoming optical pulse for some combinations, therefore the optical pulse may not experience a phase shift corresponding to the peak voltage being applied to the modulator.

is then calculated and plotted in the lower plot of figure 4.18, where the resulting phases from each sweep no longer drift. The mean phase value corresponding to each attenuator setting is then calculated and detailed in table 4.1.

The plots in figure 4.18 show that the phase of the pseudo QKD signal clearly varies with the applied attenuator combinations. However, for some attenuator settings, the calculated phase shift does not appear to correspond to the applied peak voltage. For example, the attenuator setting Att. 4, indicates no phase change, comparable to the no signal applied case. In addition, the peak voltage applied in the Att. 5 setting, although less than that in the Att. 4 setting, results in a larger phase shift. The most likely reason for this is that, as more electrical attenuators are added, the more the voltage signal is shifted with respect to the optical pulses. Therefore, as the Att. 4 setting includes 4 attenuators, the voltage impulse may simply be applied after the optical pulse has propagated through the modulator.

In addition to this, the final sweep of the piezo voltage, shown in figure 4.18, where no signal is applied to the phase modulator indicates that the phase of the pseudo QKD signal evolves over the sweep. This is most likely due to thermal effects within the phase modulator, as the modulator stabilises after the applied voltage signal is removed. This trial experiment indicates the ability of the measurement system to detect the phase changes within the pseudo QKD signal, however the generation of the pseudo QKD signal could be improved.

4.3.2 Bright & Dim Pseudo QKD Signal Experiment

To further the trial pseudo QKD signal experiment, the setup in figure 4.19 is constructed. The generation of the pseudo QKD signal consists of the PicoQuant pulsed laser [71], generating a pulse train with a temporal separation of $\sim$ 100 ns, at a wavelength of 1549.512 nm and a pulse full width half maximum of $\sim$ 117 ps. The pulse train is once

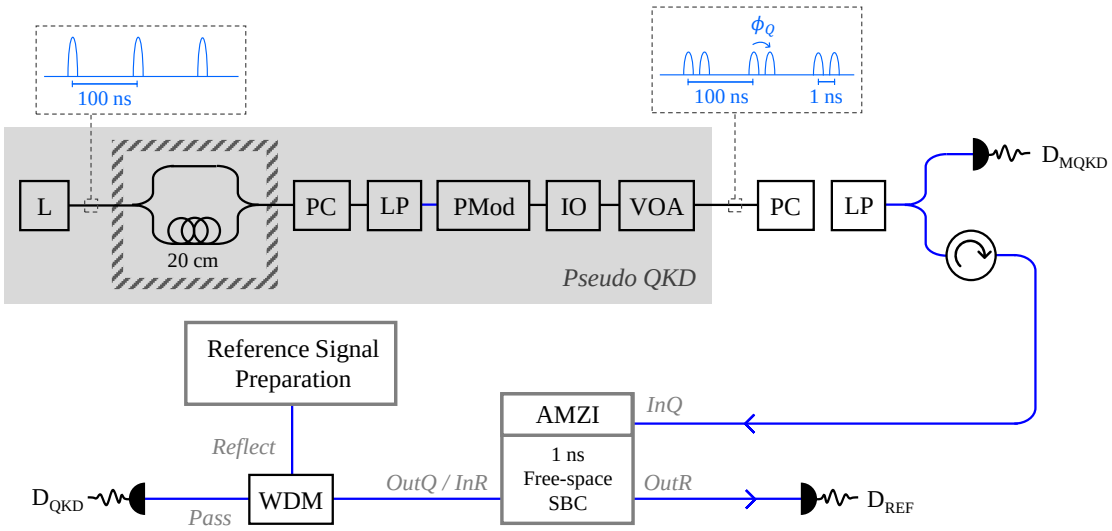


Figure 4.19: Experimental setup used to characterise a pseudo QKD signal consisting of a pulsed laser (L), a passively insulated fibre AMZI (dashed box), polarisation controls (PC), a linear polariser (LP), a phase modulator (PMod), an isolator (IO), a variable optical attenuator (VOA), a 50:50 fibre coupler, a circulator (circular arrow), the measurement system AMZI, a wavelength division multiplexer (WDM), reference signal preparation and detectors (D_{MQKD}, D_{QKD}, D_{REF}). Black lines represent single mode fibre and blue lines represent polarisation-maintaining single mode fibre. The grey shaded area indicates the devices used to generate the pseudo QKD signal and the dashed boxes at the top of the diagram represent the optical pseudo QKD signal at points within the system.

again sent into a passively insulated fibre AMZI (section 2.3.2), with an OPD of 20 cm, generating pairs of pulses with a temporal separation of ~ 1 ns. The pulse pairs are then passed into polarisation controls, a linear polariser, a phase modulator that generates a phase difference between the two pulses in the pair of ϕ_Q, an isolator and a variable optical attenuator. The outputted pseudo QKD signal is then sent through another set of polarisation controls, a linear polariser and a 50:50 coupler, where half the signal is sent to the monitoring power meter D_{MQKD} and the other half of the signal is sent into a circulator and then into the measurement system AMZI. The pseudo QKD signal output from the AMZI is sent through a wavelength division multiplexer and is then detected by D_{QKD}, which is either a power meter or the ID210 single-photon detector (SPD). The WT-MINT is set to the tap-enabled state, with a free-space OPD ($\sim$ 1 ns) containing the Soleil-Babinet compensator. The inclusion of polarisation controls and the linear polariser here, prior to the phase modulator (Thorlabs LN53S-FC), should improve the phase modulation of the optical signal in comparison to the previous trial experiment.

The two polarisation states of the reference signal are prepared, where the CW Rio Orion laser [73] is once again used for the signal with a peak wavelength of 1542.1 nm. The reference signal is sent into the AMZI via the reflect port on the wavelength division multiplexer[3] and is detected using a power meter D_{REF} at *OutR*.

The Tektronix AWG70001A arbitrary waveform generator [78] is used to generate the voltage signal supplied to the phase modulator, where the signal is amplified prior to

[3]As discussed previously, the input of the reference signal into the AMZI via the multiplexer here is operationally identical to the previous experimental setups shown where the reference signal was input via a separate port.

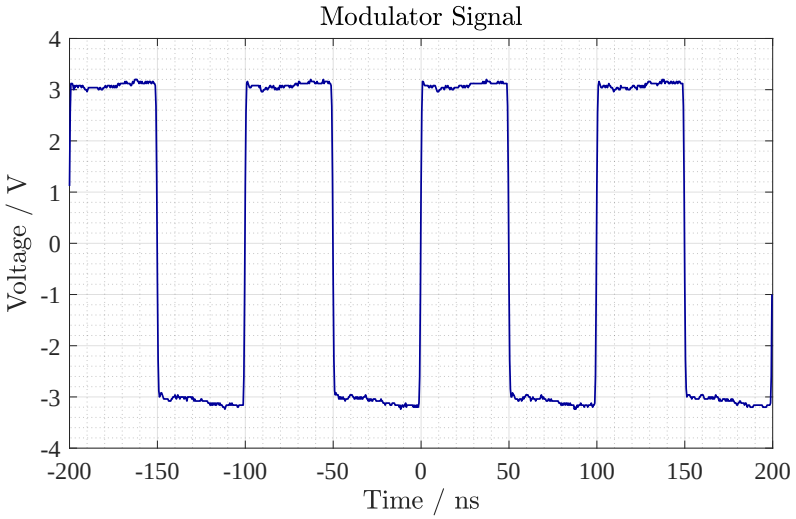


Figure 4.20: Trace of the amplified voltage signal supplied to the phase modulator.

application. Another signal from the waveform generator is also used to trigger the pulse generation of the pulsed laser, such that the voltage signal can be adjusted to arrive at the modulator at the same time as one of the pulses in the pulse pair. For the experiment performed at the single-photon level, the arbitrary waveform generator is also used to trigger the clock count of the ID210 SPD. The amplified voltage signal applied to the phase modulator is shown in figure 4.20, which is a square wave. The frequency of the square wave signal is equivalent to the laser pulse repetition rate, 10 MHz.

Bright Signal

The experiment is initially carried out using relatively bright signals, where the monitoring power of the pseudo QKD signal is 94 nW, and the slow and fast polarisation of the reference signal have an input power of 1.1 μW and 300 nW respectively. A trace of the detected pulse train of the pseudo QKD signal after passing through the measurement system is shown in the top plot of figure 4.21. The bottom plot of the same figure shows a trace of a trio of pulses, which result from a pulse pair travelling through the measurement system AMZI. The leftmost pulse results from the first pulse travelling through the short arm of the AMZI, the rightmost pulse results from the second pulse travelling through the long arm of the AMZI, and the centre pulse is a combination of the first pulse travelling through the long arm and the second pulse travelling through the short arm, such that they overlap and interfere. The piezo voltage is adjusted and traces showing full constructive and destructive interference of the centre pulse are shown in figure 4.21.

Sweeps of the piezo element are performed, varying the voltage between 0 V and 70 V with an incremental step of 1 V. Five sweeps are performed when no signal is applied to the phase modulator, and another five sweeps are performed when the voltage signal shown if figure 4.20 is applied to the modulator. The power ratios for these piezo sweeps are shown in figure 4.22, where the application of the voltage signal to the phase modulator has a clear impact on the transmittance of the pulse pair.

The change in the interferometer phase experienced by the QKD wavelength, $\Delta\theta_{IntQ}$, is calculated using the reference signal, which in turn is used to calculate the relative phase difference between the incoming pulses in the pulse pair, $\Delta\phi_Q$. For no signal applied to the phase modulator, the resulting values of $\Delta\phi_Q$ from the first five piezo sweeps are shown in figure 4.23.

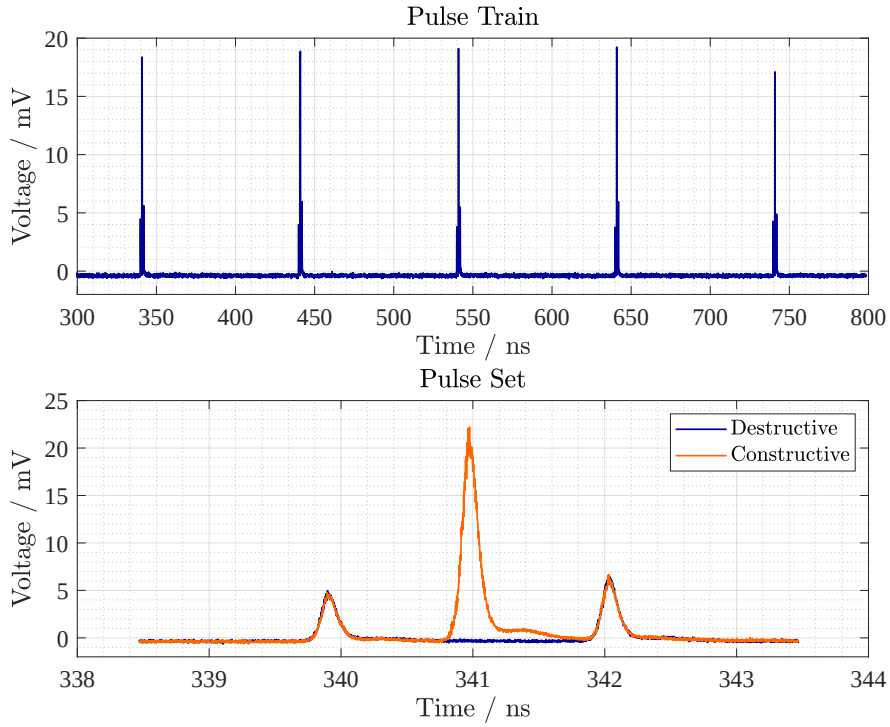


Figure 4.21: Traces of the pseudo QKD pulses after they have passed through the AMZI. The top plot shows five sets of interfering pulses in the pulse train. The bottom plot shows one of the interfering sets, where the piezo voltage has been varied to produce traces showing full constructive and destructive interference of the centre pulse. These traces are averaged over 64 recorded pulses.

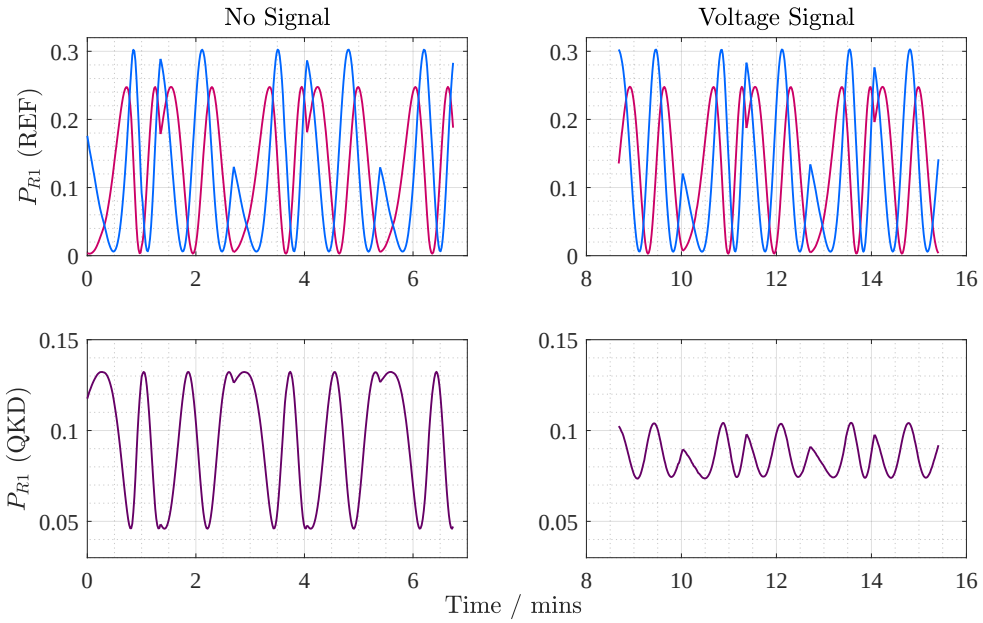


Figure 4.22: Interference patterns of the power ratio of the reference signal and the pseudo QKD signal, when no signal is applied to the phase modulator and when the voltage signal is applied to the modulator.

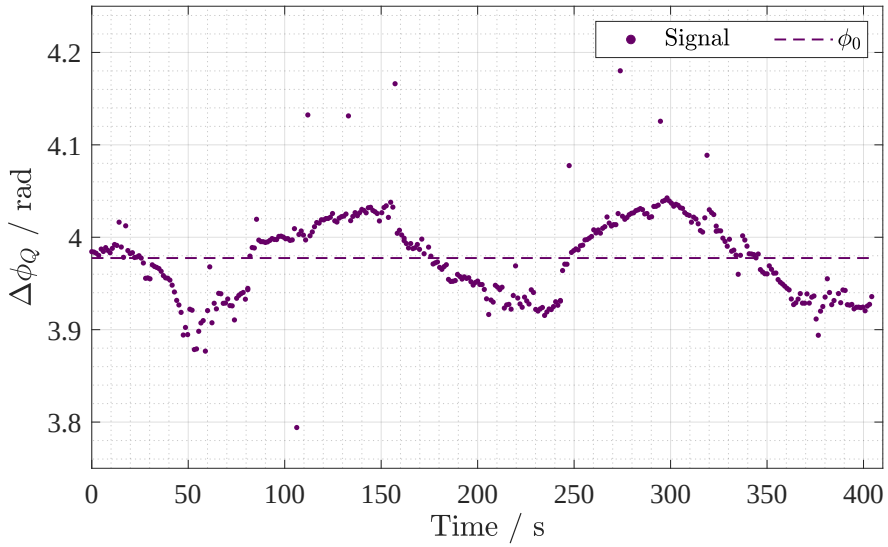


Figure 4.23: Calculated values for the phase of the pseudo QKD pulses $\Delta\phi_Q$ for the first five sweeps where no signal is applied to the phase modulator. A straight line, ϕ_0, is fitted to the data using the least square method to model the drift in the OPD of the fibre AMZI.

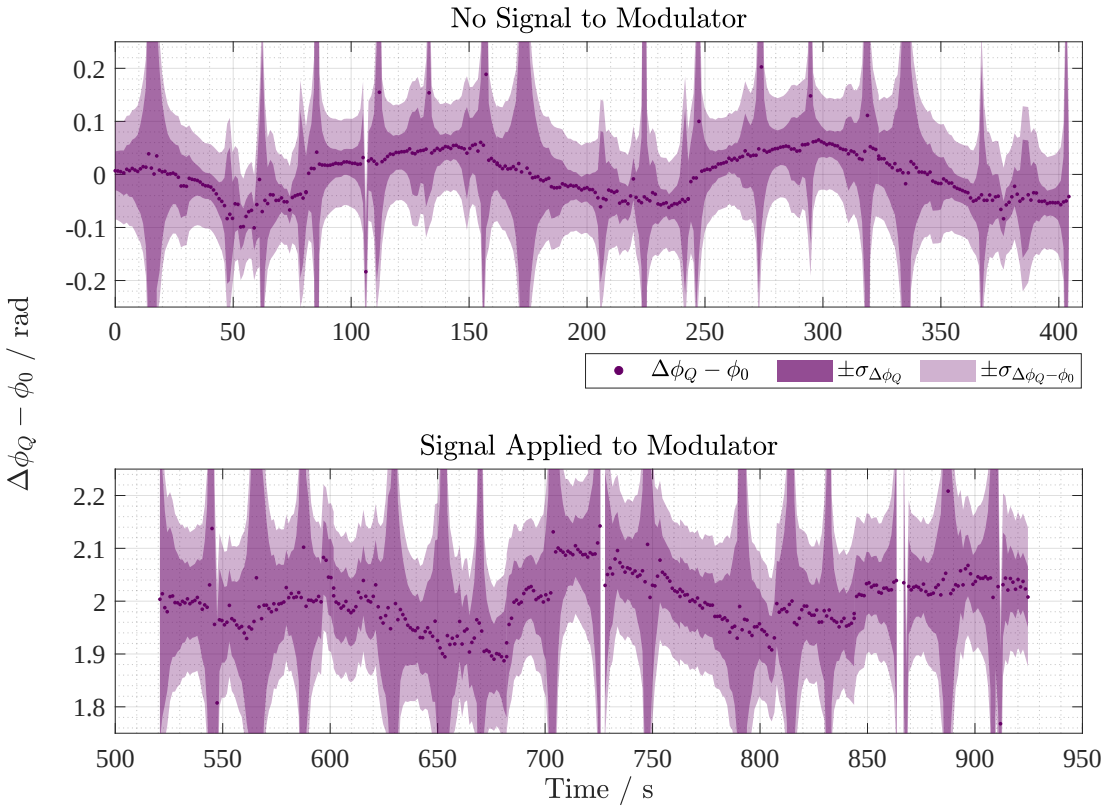


Figure 4.24: Corrected phases, $\Delta\phi_Q - \phi_0$, for the pseudo QKD signal when no signal is applied to the phase modulator and when the voltage signal is applied to the modulator. Gaps shown in the data set result from a break between the end of a piezo sweep and the start of the next, where the data analysis method only incorporates the data points taken during the piezo sweeps.

Once again, the drift in the OPD of the optical fibre AMZI used to generate the pulse pairs can be seen. A straight line, ϕ_0, is fit to these values of $\Delta\phi_Q$ using the least squares method and is extrapolated out over the measurement duration. The difference between $\Delta\phi_Q$ and ϕ_0 is then used to give the calculated phase corrected for the fibre AMZI drift. The corrected phases for the entire measurement are shown in figure 4.24. These plots contain a darker shaded region indicating the uncertainty in the measured QKD phase, $\sigma_{\Delta\phi_Q}$, and the lighter shaded region indicating the uncertainty in the drift corrected QKD phase, $\sigma_{\Delta\phi_Q-\phi_0}$. The process of correcting the drift of the fibre AMZI used in the pseudo QKD signal generation notably increases the uncertainty of the phase measurement, when compared to the uncertainty resulting from the measurement system and the pseudo QKD signal alone. For the five sweeps of the no signal and signal applied cases, the weighted mean of the corrected QKD phase is given by,

$$\text{No Signal Applied: } \Delta\phi_Q - \phi_0 = 0.00 \pm 0.15 \text{ rad}$$
$$\text{Signal Applied: } \Delta\phi_Q - \phi_0 = 1.99 \pm 0.20 \text{ rad}$$

where the weightings are proportional to the inverse square of the phase uncertainties. The assessment performed here using the measurement system has revealed that the application of the voltage signal to the phase modulator results in an average phase change in the bright pseudo QKD signal of 1.99 rad. The next step is to demonstrate this using a single-photon level QKD signal.

Single-photon Level Signal

The same measurement described above is conducted for a dim pseudo QKD signal, using the setup shown in figure 4.20. The variable optical attenuators in the pseudo QKD signal generation setup and the reference signal preparation element are used to attenuate both signals down so that the experiment can be conducted in the single-photon regime. For this experiment the ID210 SPD is used as the QKD output detector, D_{QKD}, where the SPD has a clock rate of 10 MHz, a dead time of 40 μs, a detection efficiency of 25% and a dark count rate of $\sim$ 200 Hz. The monitoring power of the pseudo QKD signal detected at D_{MQKD} is 13.78 pW, which is equivalent to 10.75 photons per pulse. This value is higher than the mean photon number per pulse required by QKD protocols, where a mean photon number less than one is typically desired. The reason for the higher power pseudo QKD signal used here is due to the monitoring power meter for the QKD signal. This power meter has a noise floor of $\sim$ 300 fW, and for the purposes of the phase measurement in this experiment, accurately monitoring the pseudo QKD signal input power is preferred over operation at a mean photon number per pulse less than one.

Due to the dead time setting of the SPD, the maximum count rate of the detector is 25 kHz. Therefore, to avoid saturation of the detector, a fixed attenuator is placed prior to the SPD input and figure 4.25 shows the recorded counts over one sweep of the piezo voltage. The resulting maximum and minimum detected mean photon number per pulse are $\sim$ 0.015 and $\sim$ 0.005. The monitoring powers of the slow and fast polarisation states of the reference signal are set to 717 nW and 193 nW respectively.

Five sweeps of the piezo voltage are performed when no signal is applied to the phase modulator and when a voltage signal is applied to the phase modulator. A straight line (ϕ_0) is fit to the calculated phase datasets of the first five sweeps (no signal applied to the modulator) using the least squares method. The resulting function is extrapolated over the measurement duration and subtracted from the calculated phase values to correct for the phase drift in the fibre AMZI. The corrected phases are shown in figure 4.26, along with shaded regions indicating the uncertainty in the measured QKD phase $\sigma_{\Delta\phi_Q}$ (darker shaded region), and the uncertainty in the drift corrected QKD phase $\sigma_{\Delta\phi_Q-\phi_0}$ (lighter

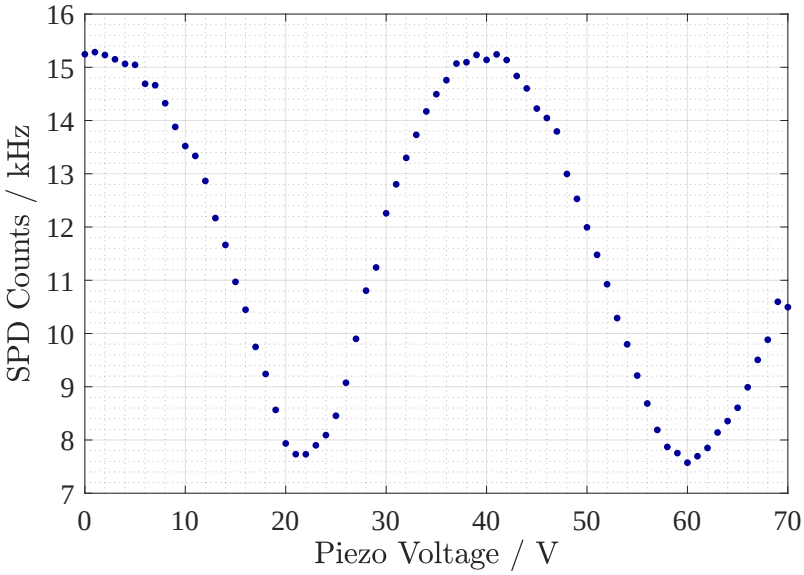


Figure 4.25: Counts detected at the ID210 SPD (D_{QKD}) for one sweep of the piezo voltage.

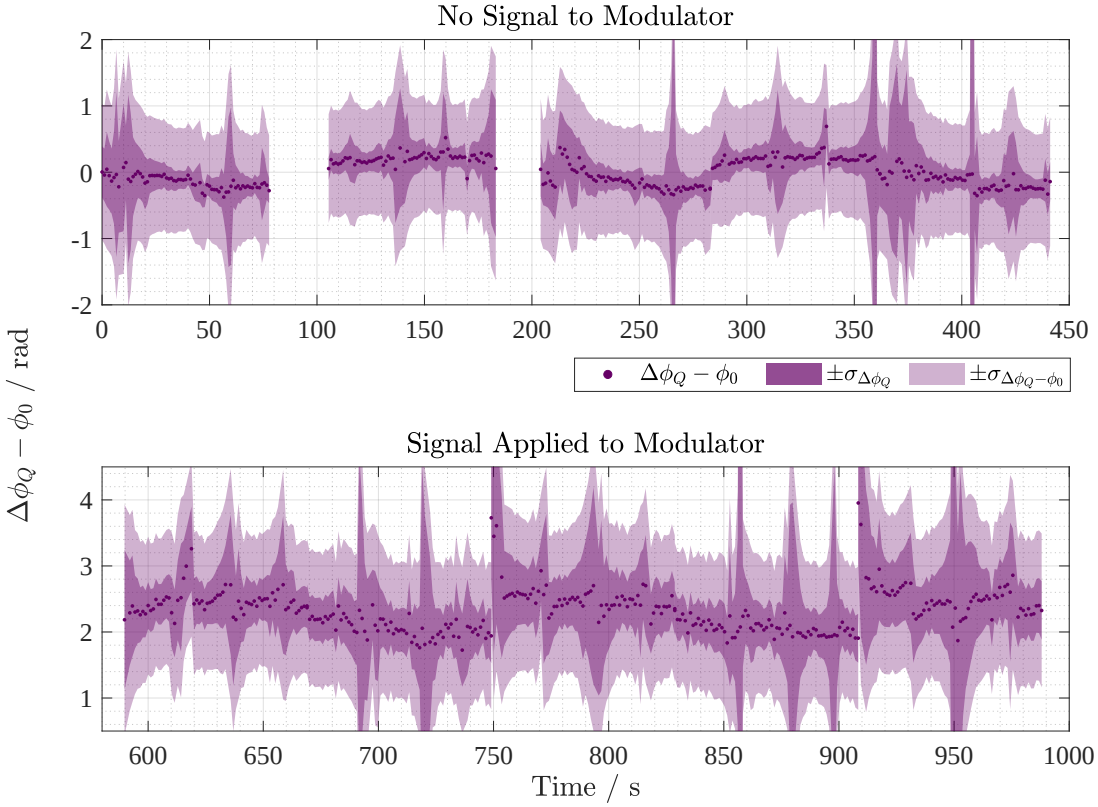


Figure 4.26: Corrected phases, $\Delta\phi_Q - \phi_0$, for the dim pseudo QKD signal when no signal is applied to the phase modulator and when the voltage signal is applied to the modulator. Once again, gaps in the dataset result from a break between the end of a piezo sweep and the start of the next, where the data analysis method only incorporates the data points taken during the piezo sweeps.

shaded region). The weighted mean for each dataset is taken and the resulting calculated phases for the two cases are given by,

$$\text{No Signal Applied: } \Delta\phi_Q - \phi_0 = -0.01 \pm 0.91829 \text{ rad}$$
$$\text{Signal Applied: } \Delta\phi_Q - \phi_0 = 2.31 \pm 1.178 \text{ rad}$$

where the weightings are again proportional to the inverse square of the phase uncertainties. The application of the voltage signal to the phase modulator results in an average change to QKD phase $\Delta\phi_Q$ of 2.32 rad. This is slightly higher than that calculated in the bright pseudo QKD signal case, however it is well within the stated uncertainty ranges. The quoted uncertainties for these final phase values are higher than anticipated. This is partly due to the corrections performed to remove the phase drift imparted by the fibre AMZI over the course of the measurement. In addition to this, improved uncertainty calculations could be developed to reduce these final stated values. For example, disregarding the phase values with higher uncertainty, near the peaks and troughs of the interference patterns, when calculating the mean phase values [47].

4.4 Trial Assessment Summary

This chapter has explored the application of the measurement system in measuring the phase of CW laser sources, the incoherence of laser pulses and the phase measurement of a pseudo QKD signal, both bright and at the single-photon level. These experiments have demonstrated the functionality of the system and the test procedures that can be used to perform phase characterisation measurements. The following work will look to apply the test procedures detailed here when characterising a prototype QKD component.

Chapter 5

Assessment of a Prototype QKD Device

5.1 Prototype QKD Component

The measurement system is designed so that it can be used to characterise both QKD transmitter and receiver modules. The characterisation of transmitter modules involves overlapping and measuring the interference of pulses from the emitted QKD pulse train. The characterisation of a receiver involves combining the measurement system with a laser source to produce a probe signal, with known phase properties, that can be sent into the receiver. This signal can then be detected, even by detectors contained within the module, and the resulting data can be used to extract information about the phase properties of the receiver.

For this work, a prototype chip-based component for a QKD system was available for characterisation. The device primarily consists of an asymmetric Mach-Zehnder interferometer (AMZI) with an optical path difference (OPD) between the two interferometer arms approximately equivalent to 500 ps. The AMZI OPD is controlled via a heating element, and power-balancing symmetric Mach-Zehnder interferometers are used before and after the AMZI. The voltage applied to the heater of the AMZI is adjusted to vary the path asymmetry in the device. The temperature of the chip is controlled using a Thorlabs TED200C temperature controller [79].

As the prototype device is not a full QKD module, it can be applied to a variety of experiments to convey the functionality of the measurement system. The device can be combined with detectors to be used as a QKD receiver and it can be used in conjunction with a pulsed laser source to produce a QKD signal. This chapter explores these two experimental formulations and demonstrates the operation of the measurement system.

5.2 Assessment of a Prototype Transmitter Signal

To generate a QKD transmitter signal using the prototype device, pulsed laser light is sent through the chip. The PicoQuant LDH-P-F-N-1550 pulsed laser [70] and the PDL 800-D laser driver [71] are used, producing light with with a peak wavelength of 1549.512 nm (optical spectrum shown in figure 3.21 in chapter 3), a pulse full width half maximum of ~ 150 ps and a pulse repetition rate of 40 MHz. This results in a pulse train with a 25 ns temporal separation between pulses. Propagating this light through the prototype device produces a train of pulse pairs, where the pulses in each pair are separated by 500 ps and have a phase difference of $\Delta\phi_Q$, due to the phase difference between the arms of the on-chip AMZI. Figure 5.1 describes the setup used to generate this transmitter signal and indicates the formation of the pulse-pair train.

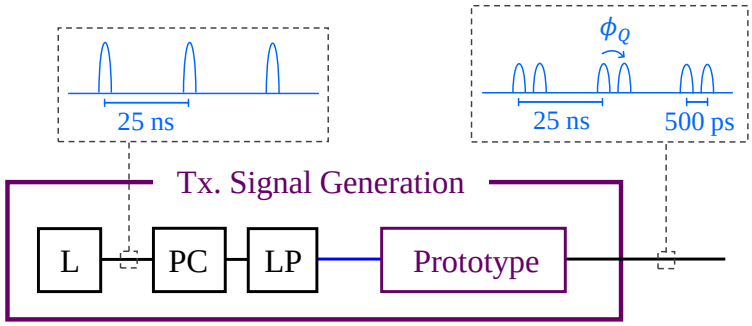


Figure 5.1: Experimental setup used to generate the transmitter signal using the prototype QKD device, consisting of a pulsed laser (L), polarisation controls (PC), linear polariser (LP) and the prototype device. Black lines indicate single mode fibre and blue lines indicate polarisation-maintaining single mode fibre. The diagrams above indicate the state of the optical signal at different stages within the setup.

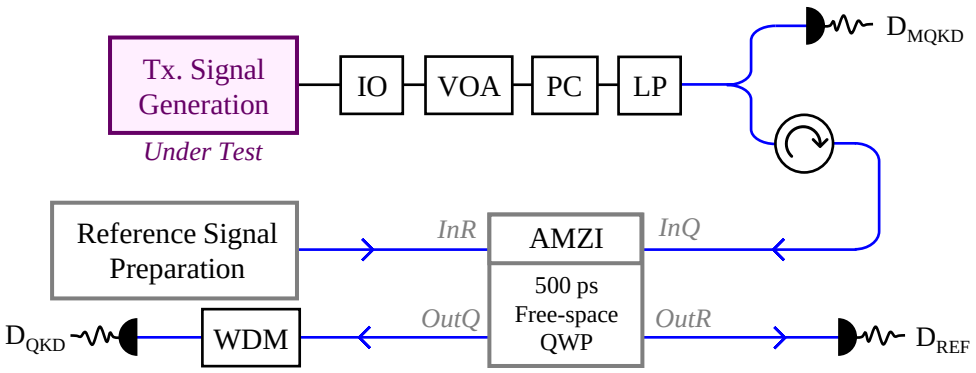


Figure 5.2: Experimental setup used to assess the transmitter signal generated using the prototype QKD device. The setup consists of the transmitter signal generation (Tx. Signal Generation), an isolator (IO), a variable optical attenuator (VOA), polarisation controls (PC), a linear polariser (LP), a circulator (circle with arrow), the measurement system AMZI, a wavelength division multiplexer (WDM) and detectors (D_{MQKD}, D_{QKD} and D_{REF}). Black lines indicate single mode fibre and blue lines indicate polarisation-maintaining single mode fibre. Details of the transmitter signal generation are shown in figure 5.1. The measurement system WT-MINT is set to the tap-enabled state with a free-space OPD extension of 500 ps containing a quarter waveplate, as shown in figure 3.6 in chapter 3. The reference signal preparation is shown in figure 3.7, also in chapter 3.

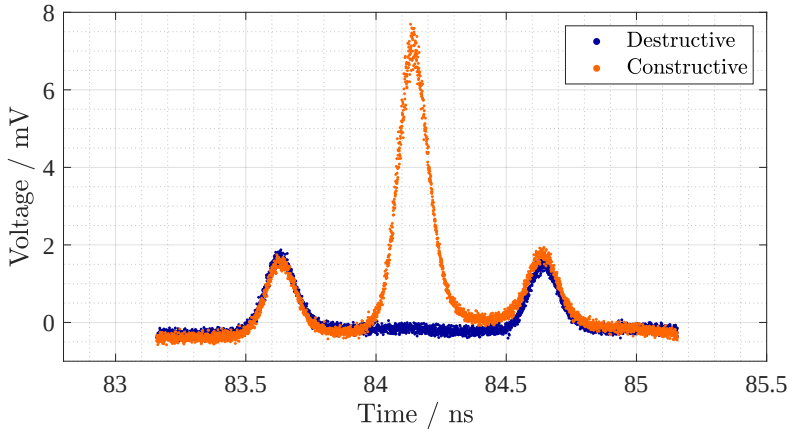


Figure 5.3: Traces of the optical pulses of the prototype device signal exiting the measurement system AMZI at output *OutQ*. The piezo voltage applied to the measurement system AMZI is adjusted to produce traces showing full constructive and destructive interference of the central pulse.

The measurement system can be used to measure the phase difference between the pulses in each pair in the signal using the setup shown in figure 5.2. The WT-MINT of the measurement system is set to the tap-enabled state, with a free-space optical extension containing a quarter waveplate (see figure 3.6 in chapter 3), resulting in an OPD of ~ 500 ps. This is equivalent to the OPD of the AMZI in the prototype device and results in the interference of the pulses in each pulse pair. A voltage setting is applied to the heater controlling the OPD of the on-chip AMZI, producing a pulse train where the phase difference between the pulses within each pair corresponds to that heater voltage setting. For each heater setting, many of the pulse pairs are measured whilst performing sweeps of the voltage applied to the piezo element within the measurement system. This is then repeated for various heater voltage settings. The variable optical attenuators in the setup shown in figure 5.2 are used to vary the intensity of the generated transmitter signal, so that experiments involving bright and single-photon level signals can be performed.

5.2.1 Initial Assessment with a Bright Transmitter Signal

Initial tests of the prototype device are performed with relatively bright transmitter and reference signals and the detectors shown in figure 5.2 are power meters. The optical power of the slow and fast reference signal are 1.2 µW and 510 nW respectively and the average power of the QKD signal is 170 nW. The generated signal from the prototype device is sent through the measurement system and the OPD of the measurement system AMZI is adjusted, so that the pulses of the incoming pulse pairs overlap and interfere. The pulses are detected at the AMZI output *OutQ* using the Thorlabs DXM30AF fast photodetector [72] and are viewed using the Agilent Infiniium DCA-J 86100C sampling oscilloscope. Traces of the pulses are shown in figure 5.3, where the voltage applied to the piezo element in the AMZI is adjusted to observe full constructive and destructive interference.

The applicable range of the heater voltage settings for the prototype device is between 0 V and V_{max}, which is supplied by a separate power supply operating in constant voltage mode. Voltages are applied to the heater and, for each setting, the piezo voltage of the measurement system is swept between 0 V and 70 V in 0.1 V increments, where each piezo sweep takes ~ 8 minutes.

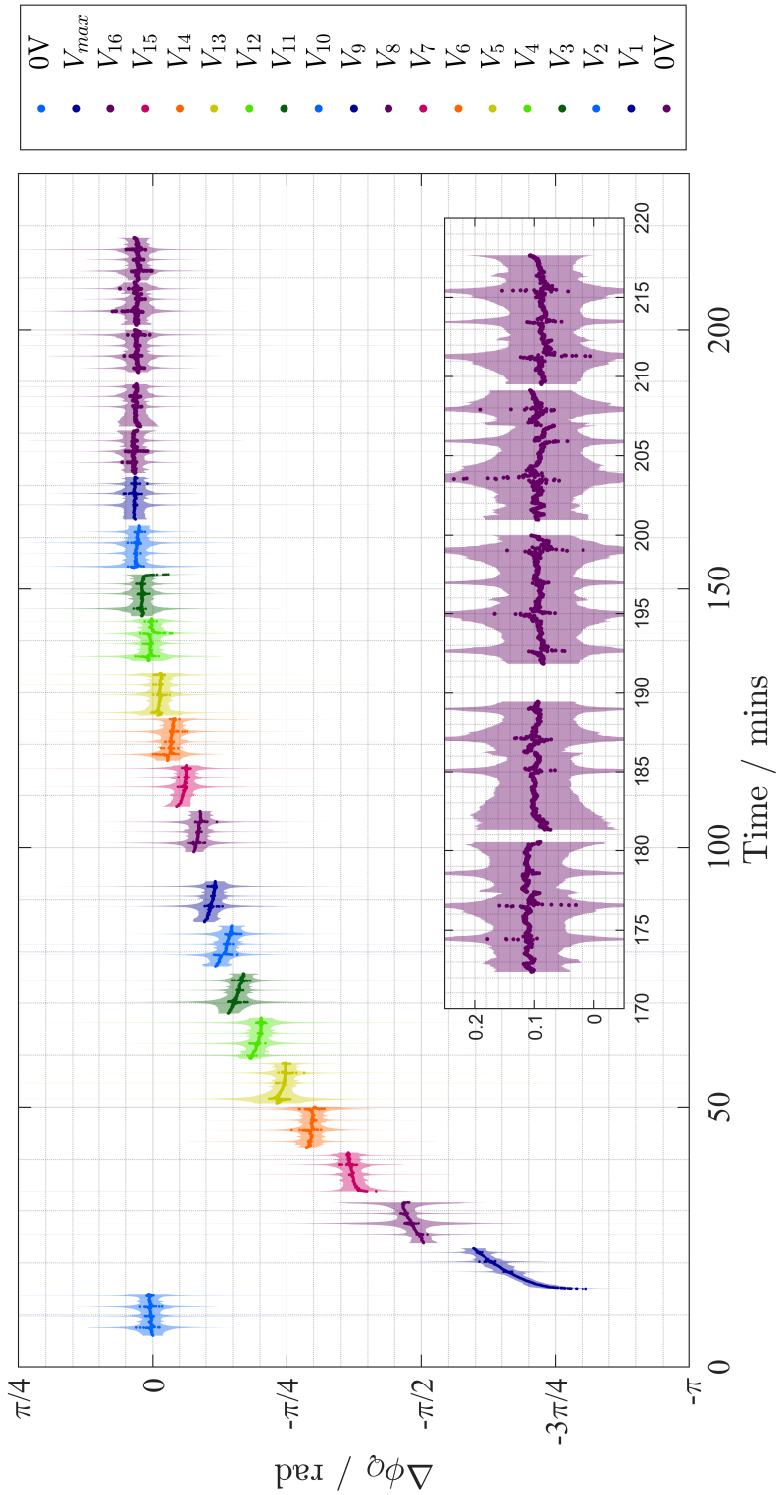


Figure 5.4: Phase between pulse pairs $\Delta\phi_Q$ over time, including both the data points and their associated measurement uncertainties (shaded regions). One sweep of the piezo voltage is performed for each voltage setting applied to the on-chip AMZI heater. The heater settings are applied in the same order as shown in the legend. The magnified plot shows the final five sweeps (sweeps 19 to 23), which are all performed for a heater voltage setting of 0 V.

Heater Setting: 0 V

Sweep Number	**Weighted Mean $\Delta\phi_Q$ / rad**
1	0.013 ± 0.072
19	0.110 ± 0.069
20	0.098 ± 0.073
21	0.091 ± 0.076
22	0.093 ± 0.078
23	0.087 ± 0.071

Table 5.1: Weighted mean of $\Delta\phi_Q$ and the associated uncertainty for the signal generated using the prototype device when the AMZI heater setting is 0 V. The values are calculated using the data sets shown in figure 5.4 and the sweep numbers correspond to the order shown in that figure.

The heater voltage, initially at 0 V, is set to V_{max} and is adjusted back down to 0 V in 17 equal voltage steps. The reference signal is used to calculate the phase difference between the two arms of the measurement system AMZI. This phase is combined with the calculated phase of the detected transmitter signal to determine the original phase difference between the pulse pairs, $\Delta\phi_Q$. The resulting calculated phases for all of the heater settings are shown in figure 5.4. The phase of each individual recorded data point across each piezo sweep is plotted, along with a shaded region indicating the corresponding measurement uncertainty, where these uncertainties are calculated using the following parameters, $\varepsilon_{Temp} = 0.1$ mrad, $\varepsilon_\lambda = 20$ mrad. On the application of higher voltages to the heating element, the calculated phase difference between the pulse pairs varies over the 8-minute piezo sweep. This is likely due to the temperature controller counteracting the heat dissipation from the heater, resulting in a slow change to the OPD of the on-chip AMZI. The final five sweeps of the piezo are performed for a heater voltage setting of 0 V, where a magnified plot of these sweeps is also shown in figure 5.4.

The weighted means of $\Delta\phi_Q$ for the 0 V heater settings are calculated. This is done for the first sweep and the final five sweeps (sweeps 19 to 23), where the weightings are proportional to the inverse square of the measurement uncertainty. These values are detailed in table 5.1, where the phase of the final sweeps at the 0 V heater setting are greater than that calculated for the first sweep. This indicates that the chip may have heated over the course of the measurement, resulting in a change to the OPD of the on-chip AMZI.

Subsequently, a second set of data is recorded where the heater voltage is swept up and down across settings V_1, V_5, V_9, V_{13}, V_{max}. A piezo sweep is performed for each of the heater settings and the resulting calculated phases and their measurement uncertainties are plotted in figure 5.5, where the uncertainties are calculated using the same values for ε_{Temp} and ε_λ. Effects of the thermal stabilisation of the chip on $\Delta\phi_Q$ can be seen, where the drift of the phase appears to be positive for the sweep up of the heater voltage and negative for the sweep down. To compare the phases for each heater setting on the sweep up and sweep down, the data sets in figure 5.5 are replotted in figure 5.6. The time of each data set is initialised to the start of the corresponding piezo sweep and the plots are separated for the different heater voltage settings.

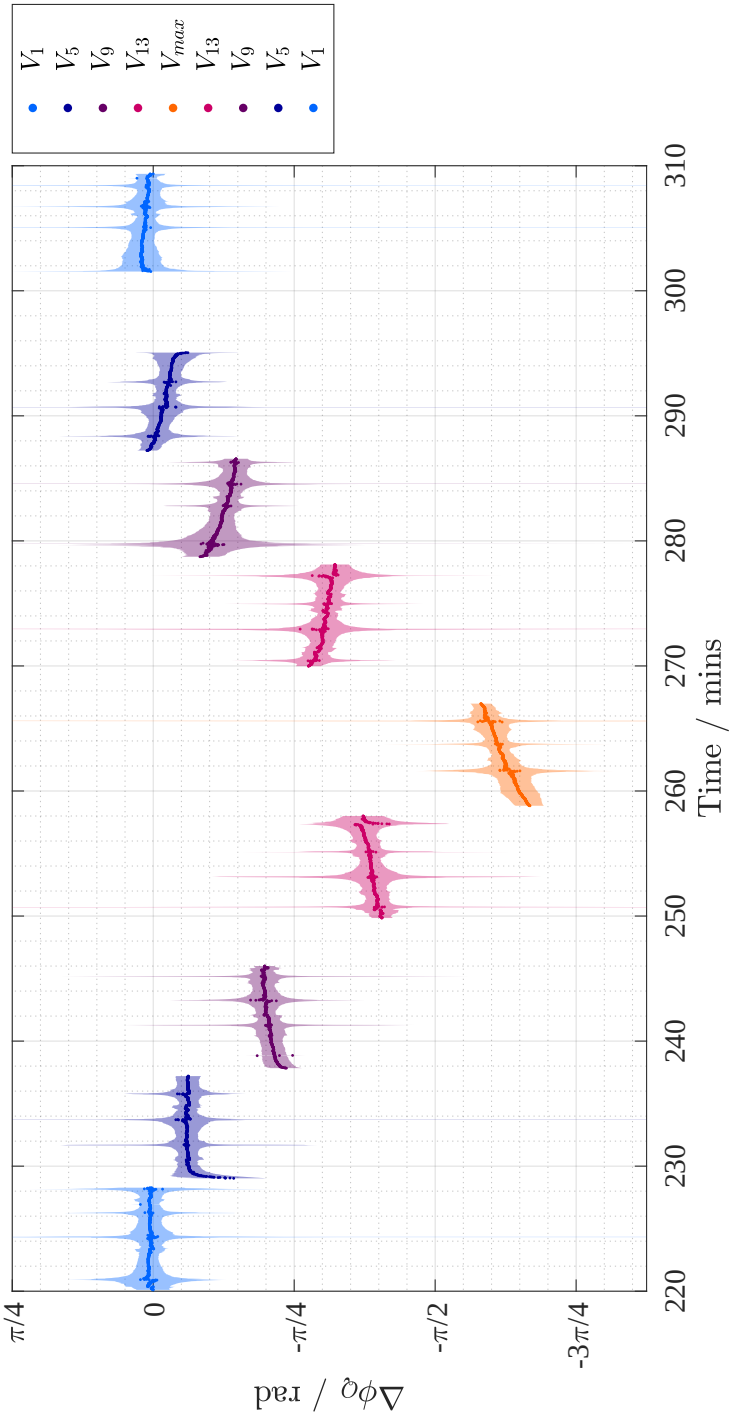


Figure 5.5: Calculated transmitter phases $\Delta\phi_Q$ for a sweep up and sweep down of the heater voltage settings V_1, V_5, V_9, V_{13} and V_{max}. At each heater setting the piezo voltage is swept between 0 V and 70 V in increments of 0.1 V.

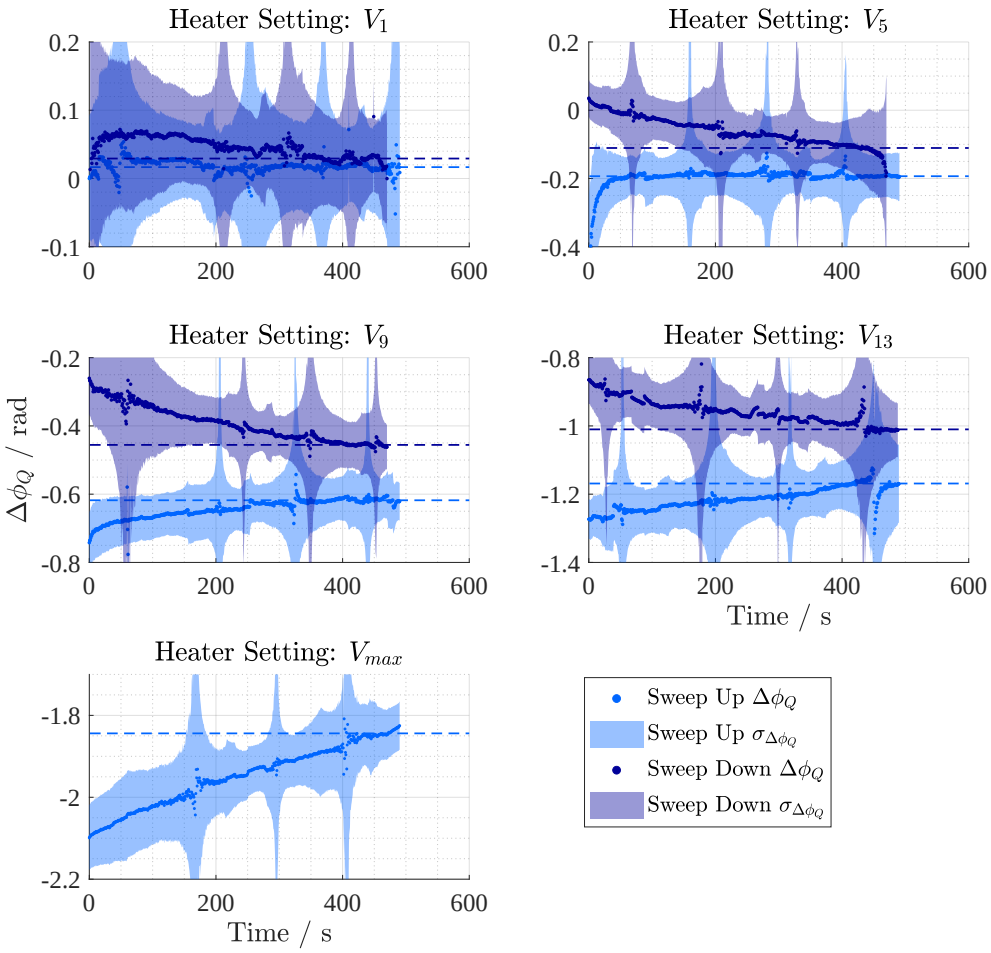


Figure 5.6: Phases shown in figure 5.5 are replotted, where each plot shows the measured phases associated with one heater voltage setting. Sweep up and sweep down refer to the heater voltage sweep directions. The dashed lines indicate the weighted mean value of the last 100 points ($\sim$ 70 s) of each data set.

Heater Voltage Setting	**Sweep Up $\Delta\phi_Q$ / rad**	**Sweep Down $\Delta\phi_Q$ / rad**
V_1	0.017 ± 0.076	0.029 ± 0.068
V_5	-0.193 ± 0.067	-0.111 ± 0.095
V_9	-0.618 ± 0.074	-0.456 ± 0.080
V_{13}	-1.169 ± 0.136	-1.010 ± 0.115
V_{max}	-1.844 ± 0.069	n/a

Table 5.2: Weighted mean phase values of the final 100 data points of each data set shown in figure 5.6 above.

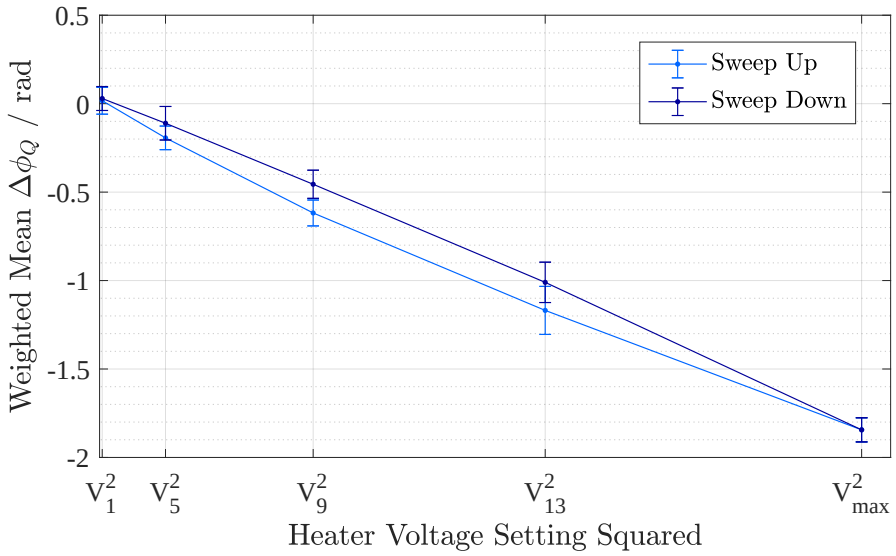


Figure 5.7: Plots of the weighted mean values of $\Delta\phi_Q$ as shown in table 5.2 for the sweep up and sweep down of the heater voltage across settings V_1, V_5, V_9, V_{13} and V_{max}.

To provide an estimate of the phase difference $\Delta\phi_Q$ corresponding to the heater voltage settings, the weighted mean of the final 100 points, equivalent to ~ 70 s, of each sweep is calculated and also plotted in figure 5.6. These averages and their associated uncertainties are detailed in table 5.2 for both the sweep up and sweep down of the heater voltage. From the plots shown in figure 5.6, the weighted average values of the phase appear to provide a good estimate for the phase value of the heater settings V_1, V_5, V_9, V_{13}, V_{max}. However, the phase for the V_{max} setting does not appear to stabilise across the piezo sweep, which is also seen in figure 5.4 for the previous dataset. This is once again most likely due to the temperature control of the chip, as it may not be able to adequately counteract the heat dissipated by the V_{max} heater setting. For the other four heater settings, some evidence of hysteresis can be seen in the weighted mean values of the phase. This is clearly demonstrated in figure 5.7, where the weighted mean of $\Delta\phi_Q$ is plotted against the heater voltage setting squared. The data shows a linear correlation between the square of the voltage and the weighted mean of $\Delta\phi_Q$, particularly on the sweep down. The voltage squared is proportional to the heater power, which in turn is also approximately proportional to the on-chip temperature change [80]. The effects of hysteresis can particularly be seen for voltage settings V_9 and V_{13}, where the measurement uncertainty error bars do not overlap for the sweep up and sweep down cases.

5.2.2 Assessment with a Single-photon Level Signal

To perform an assessment of a single-photon level transmitter signal, the variable optical attenuator in figure 5.2 is used to reduce the intensity of the pulsed laser light. In the setup shown in that figure, detectors D_{MQKD} and D_{REF} are power meters, however detector D_{QKD} is replaced with the ID210 single-photon detector. The average monitoring power of the transmitter signal detected at D_{MQKD} is 5.95 pW, equivalent to a mean photon number per pulse of 1.16. For a real QKD transmitter signal the mean photon number per pulse would be < 1, however the power level of the transmitter signal is chosen so that any fluctuations in its input power can be monitored by a power meter (D_{MQKD}),

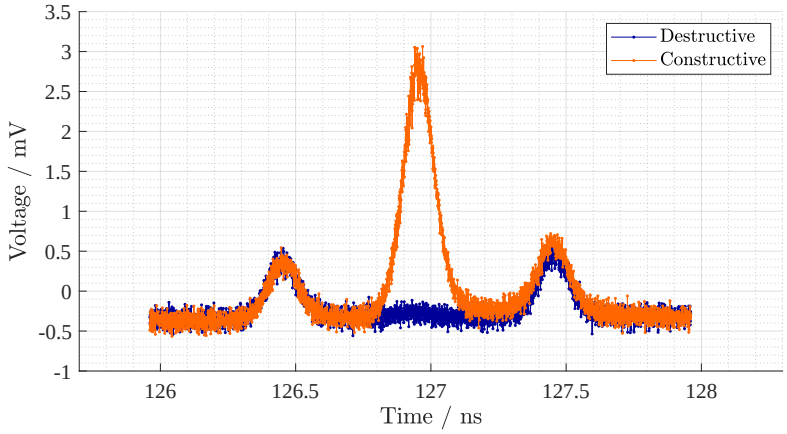


Figure 5.8: Traces of the transmitter signal pulses detected at output *OutQ* of the measurement system AMZI, where the piezo voltage is adjusted to produces traces showing full constructive and destructive interference.

where the noise floor of this power meter is ~ 300 fW[1]. The single photon detector is set to have a detection efficiency of 25 %, a clock rate of 40 MHz and a dead time of 40 µs. To avoid saturation of the single photon detector output, a fixed attenuator is placed before its input. The power of the reference signal for the slow and fast polarisations are 2.7 nW and 1.0 nW respectively.

Initially, using bright laser pulses, the measurement system AMZI is optimised to overlap the incoming pulse pairs of the signal from the prototype device. The bright pulses are detected at the measurement system AMZI output *OutQ* using the Thorlabs DXM30AF fast photodetector [72] and viewed using the Agilent Infiniium DCA-J 86100C oscilloscope. Traces of the pulses are shown in figure 5.8, where the piezo voltage is adjusted to show full constructive and destructive interference. The power of the pulsed signal from the prototype device is then reduced significantly using the variable optical attenuator. For a heater voltage setting of 0 V, a sweep of the piezo element in the measurement system between 0 V and 70 V in increments of 0.1 V is performed. The resulting counts detected by the SPD are shown in figure 5.9, where the peaks of the interference pattern are wider than the troughs due to the varying number of gates available for detection, as described in section 3.3.4. The maximum number of counts possible is 25 kHz, due to the detector dead time of 40 µs. The resulting minimum and maximum mean photon number per pulse detected by the SPD are 7.4×10^{-4} and 4.1×10^{-3}. These mean photon numbers are low to avoid saturation of the detector, given the long dead time set to negate the effects of afterpulsing.

A similar experimental procedure to that performed for the bright prototype device signal is also carried out here. The voltage applied to the heater is swept up and down the heater settings 0 V, V_4, V_8, V_{12}, V_{16}. Two sweeps of the piezo element are performed for each heater setting, except for the 0 V heater setting where four sweeps are performed. The piezo voltage sweeps are between 0 V and 70 V in increments of 0.1 V and each sweep takes $\sim$ 14 minutes. The heater voltage setting of V_{max} is not included in these sweeps in an attempt to avoid the thermal stabilisation issues of the chip seen in the previous experiments. The calculated phase of the transmitter signal is shown in figure 5.10. Drift in the calculated phase $\Delta\phi_Q$ can be seen across the piezo sweeps, where this drift appears to be increasing on the sweep up and decreasing on the sweep down. The drift is also more

[1]A second single-photon detector could instead be used for measurements on a real QKD transmitter, but this was not available for this experiment.

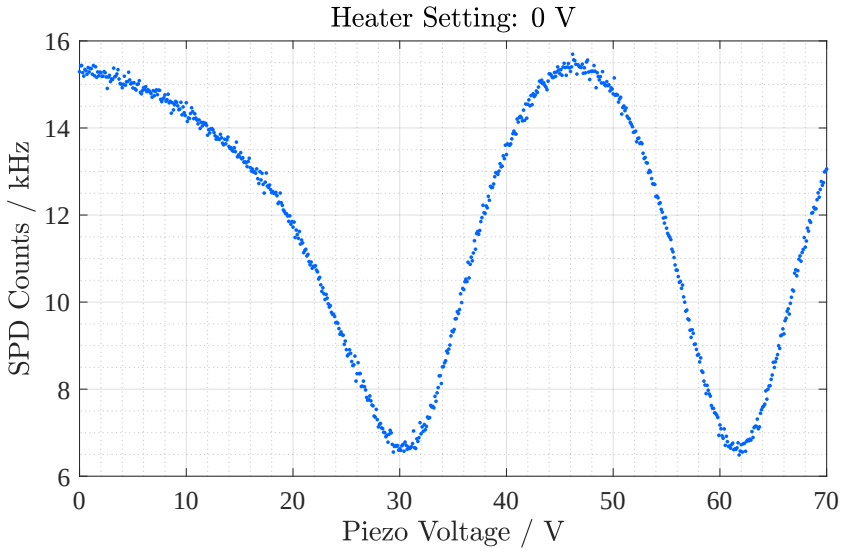


Figure 5.9: SPD counts of the prototype device signal detected at D_{QKD} in figure 5.2. The voltage applied to the piezo element of the measurement system is varied resulting in an interference pattern, where the peaks of the pattern are wider than the troughs due to the varying number of gates available for detection.

significant for higher voltage heater settings and is more pronounced on the sweep down of the heater voltage. This indicates that the thermal stabilisation of the chip is affecting the OPD of the AMZI within the receiver. However, by performing at least two sweeps of the piezo for each heater setting, the phase is given more time to stabilise and may allow for a better estimate of the phase associated with each heater voltage.

The datasets shown in figure 5.10 are replotted in figure 5.11, where the sweeps are grouped according to the heater voltage setting and each dataset is initialised to the start time of the first piezo sweep. All of the heater voltage settings show some stabilisation of the phase $\Delta\phi_Q$ over the piezo sweep, apart from the V_{16} setting, which continues to show drift in the phase after 30 minutes. The weighted average of the last 100 points ($\sim$ 125 s) of each dataset is calculated and shown on the plots in figure 5.11. These mean values and their associated uncertainties are also detailed in table 5.3 and plotted in figure 5.12. Some form of hysteresis can be seen in the data, however more significant is the offset between the two values of $\Delta\phi_Q$ for the 0 V heater setting on the sweep up and sweep down. This could be attributed to the the heating of the on-chip AMZI over the course of the experiment, however as the error bars for these two phase values overlap considerably, the validity of this phase offset cannot be established.

The phase shifts achieved in this experiment over the 0 V to V_{16} range are significantly less than that achieved in the previous set of experiments involving the bright transmitter signal. Using the data shown in figure 5.7 for the bright transmitter signal, an estimate for the phase difference between a heater voltage setting of 0 V and V_{16} would be $\sim$ 1.7 rad. Whereas the data shown in figure 5.12 for the single-photon level signal would estimate a phase difference between 0 V and V_{16} of $\sim$ 1 rad. This discrepancy may be due to the fact that multiple sweeps of the piezo were performed for each heater setting ($\sim$ 28 minutes) in the single-photon level data. These multiple sweeps result in the heater being left on for longer when compared to the bright-signal experiment where only one piezo sweeps was performed per heater setting ($\sim$ 8 minutes). The warming of the chip once again is likely to have caused the OPD of the AMZI to change and may have counteracted the phase shifting effects, resulting in a reduced phase change $\Delta\phi_Q$.

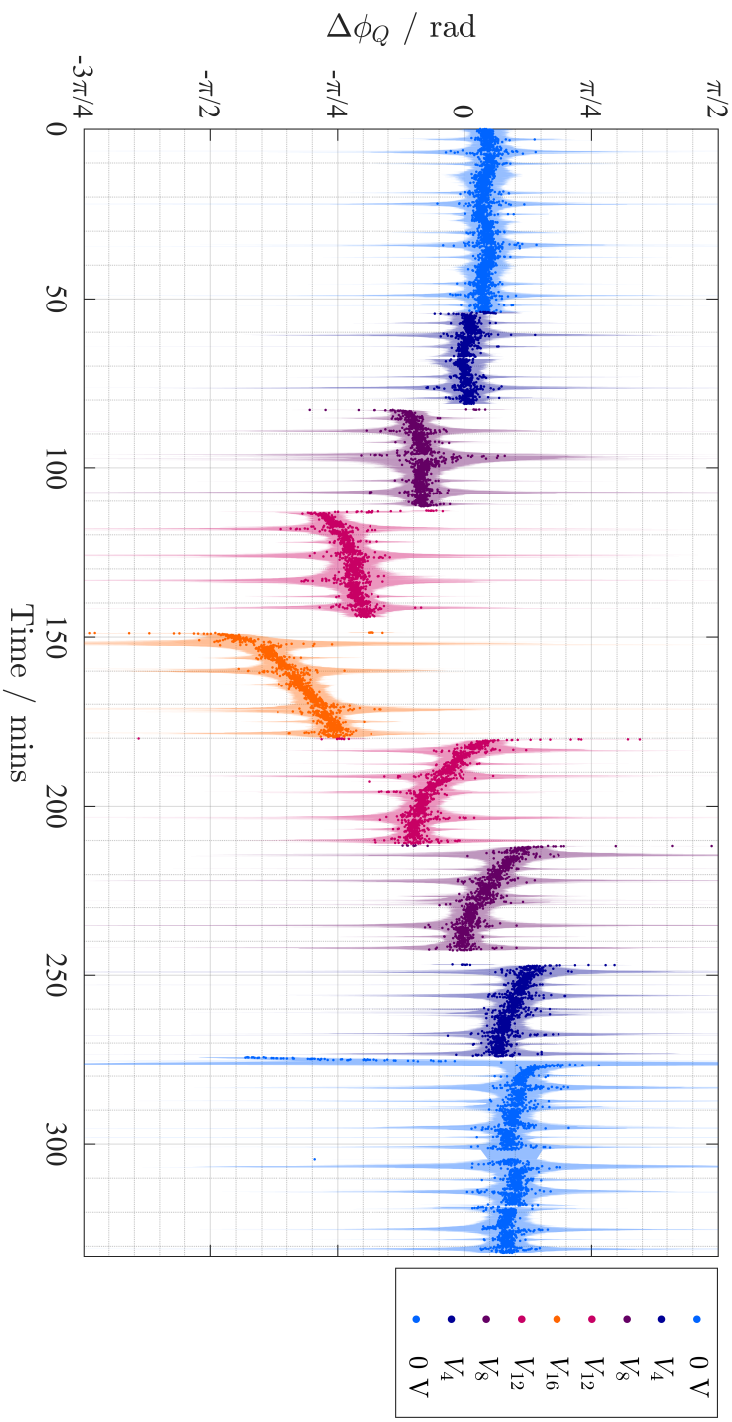


Figure 5.10: Calculated phases of the prototype device signal for sweeps of the heater voltage between settings 0 V, V_4, V_8, V_{12} and V_{16}. The order of the heater voltage settings applied is the same as the order in the legend, where two piezo sweeps are performed for every heater voltage setting, except for the 0 V settings where four piezo sweeps are performed.

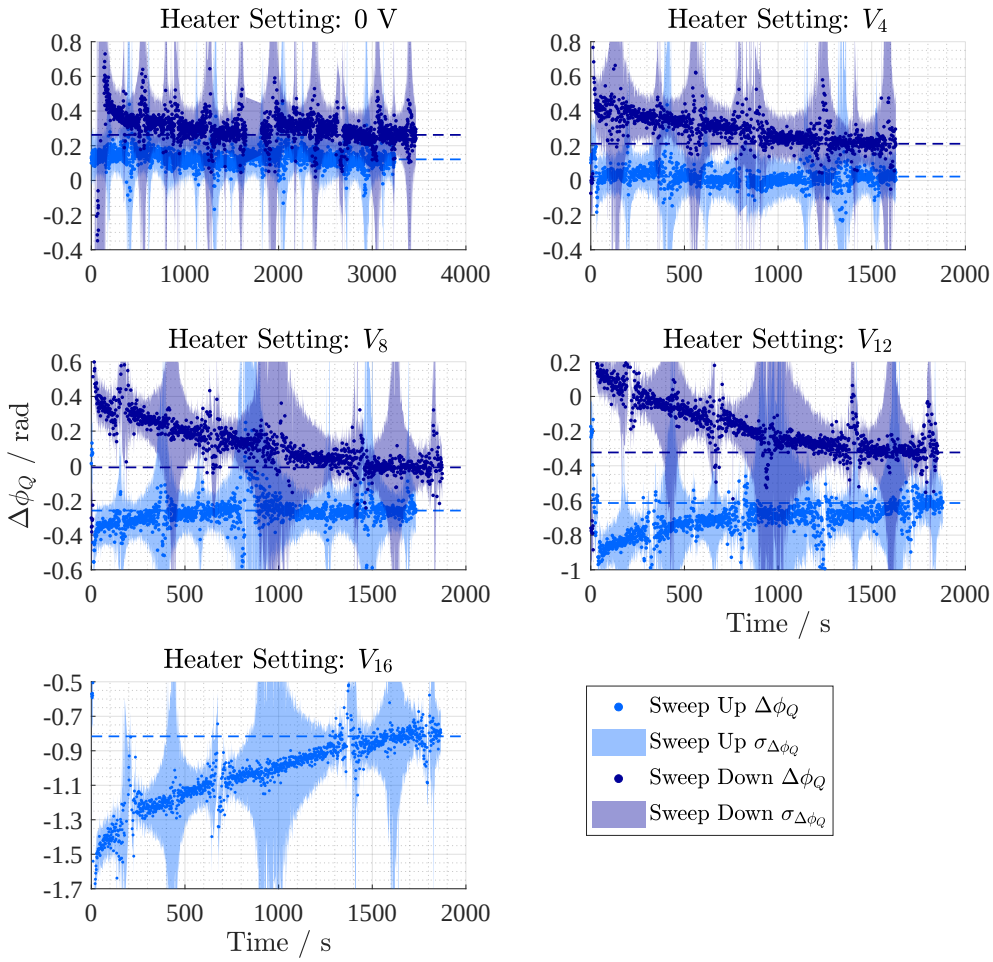


Figure 5.11: Plots of the transmitter phase $\Delta\phi_Q$ for the sweep up and sweep down of the heater voltage settings. Each plot corresponds to a different heater voltage and the time is initialised to the start of each dataset. Two sweeps of the piezo voltage are used to construct each dataset, except for the 0 V heater setting which consist of four sweeps of the piezo voltage. The weighted mean of the final 100 points, equivalent to $\sim$ 125 s, of each dataset is calculated and plotted (dashed line).

Heater Voltage Setting	**Sweep Up $\Delta\phi_Q$ / rad**	**Sweep Down $\Delta\phi_Q$ / rad**
0 V	0.121 ± 0.127	0.262 ± 0.250
V_4	0.022 ± 0.132	0.211 ± 0.214
V_8	-0.258 ± 0.128	-0.009 ± 0.125
V_{12}	-0.615 ± 0.128	-0.323 ± 0.127
V_{16}	-0.816 ± 0.128	n/a

Table 5.3: Weighted mean of $\Delta\phi_Q$ as shown in figure 5.11. The weighted mean is calculated using the final 100 points from each dataset.

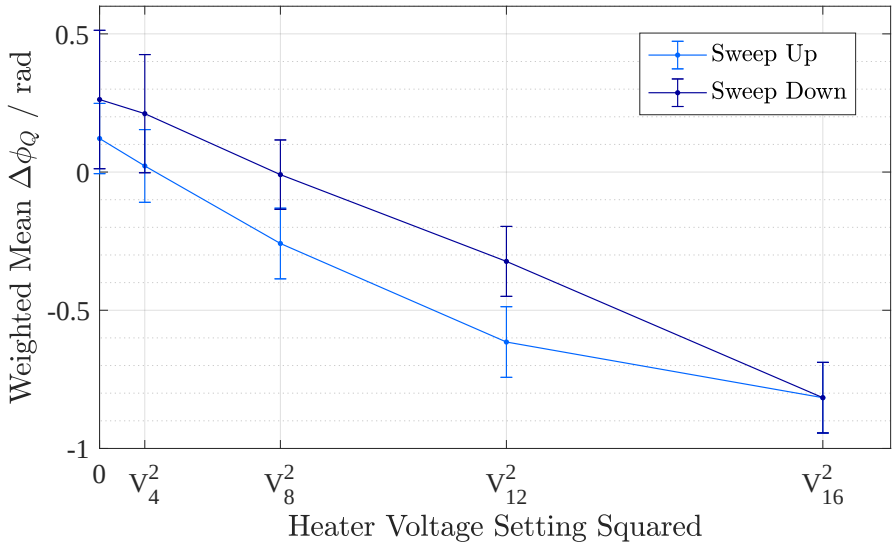


Figure 5.12: Plots of the weighted mean values of the transmitter phase as shown in table 5.3 for the sweep up and sweep down of the heater voltage across settings 0 V, V_4, V_8, V_{12} and V_{16}.

Given the effects of the chip thermal stabilisation on the phase imparted by the prototype device, it will be important to compare the phase shift applied by the different heater settings when the heater voltage is alternated at a faster rate.

5.3 Assessment of a Prototype QKD Receiver

To assess the prototype device as a receiver, it is combined with a detector, either a power meter or an SPD, and the measurement system is combined with a pulsed laser source to produce a probe signal with known phase properties. This probe signal is sent into the prototype device and the resulting output is analysed to extract information about the phase shifts imparted by the prototype. The laser source used is the PicoQuant LDH-P-F-N-1550 pulsed laser [70] with the PDL 800-D laser driver [71]. The laser light has a peak wavelength of 1549.512 nm (optical spectrum shown in figure 3.21 in chapter 3), a pulse full-width half maximum of $\sim$ 150 ps and a pulse repetition rate of 40 MHz. This produces a pulse train with a 25 ns temporal separation between pulses, which is then sent through the AMZI of the measurement system. The WT-MINT is set to the tap-enabled state, with a free-space path extension consisting of a quarter waveplate and resulting in an OPD of $\sim$ 500 ps, see figure 3.6 in chapter 3. This produces a train of pulse pairs, where the pulses in each pair are separated by 500 ps and have a phase difference of ψ_{Int}. These pulses are then sent into the prototype device, which imparts a phase shift of $\phi_{Rx.}$ and interferes the pulses in each pair. The experimental setup used to generate the probe signal and assess the receiver phase, $\phi_{Rx.}$, is shown in figure 5.13. Detectors D_{MP} and D_P are used to monitor and detect the probe signal respectively.

From the results of the previous section, which concerned the assessment of a QKD signal generated using the prototype device, the heating and thermal stabilisation of the chip had a noticeable impact on the measured phase. To further explore these features, two types of assessment are performed using the prototype receiver. The first, further assesses the long term stability of the heater and temperature control using a relatively bright probe signal. The second uses a single-photon level signal to assess the phase of the receiver when performing a faster switching routine of the on-chip AMZI heater voltage.

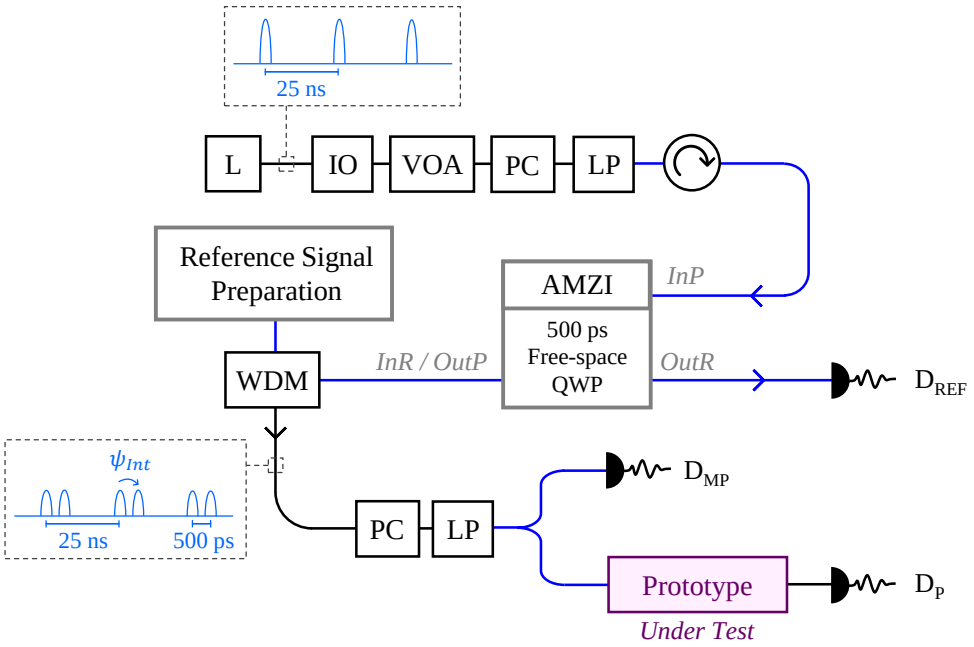


Figure 5.13: Experimental setup for characterising the prototype device as a receiver, consisting of a pulsed laser (L), an isolator (IO), a variable optical attenuator (VOA), polarisation controls (PC), a linear polariser (LP), a circulator (circle with arrow), the measurement system AMZI, the reference signal preparation, a wavelength division multiplexer (WDM), the prototype device and detectors (D_{REF}, D_{MP}, D_P). Black lines indicate single mode fibre and blue lines indicate polarisation-maintaining single mode fibre. The pulse diagrams indicate the state of the optical signal at different points within the setup.

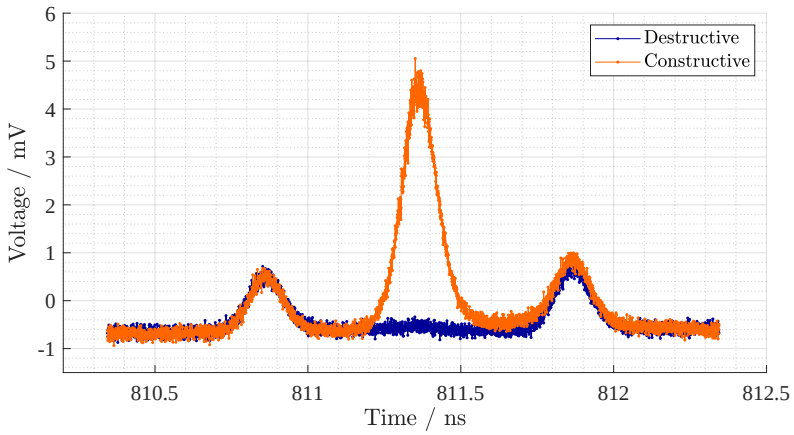


Figure 5.14: Traces of an interfering pair of pulses at the prototype device output, where the piezo voltage of the measurement system has been adjusted to show full constructive and destructive interference of the centre pulse.

5.3.1 Long Term Stability (Bright Probe Signal)

For this set of experiments, the variable optical attenuator shown in figure 5.13 is set to produce a relatively bright probe signal, with an average optical power of 2.5 nW detected at D_{MQKD}, equivalent to ~ 500 photons per pulse. The input power of the reference signal slow and fast polarisations is 1.1 μW and 400 nW respectively. Detectors D_{REF}, D_{MP} and D_P in the setup shown in figure 5.13 are all power meters. Traces of the pulses at the prototype device output are shown in figure 5.14, which are detected using the Thorlabs DXM30AF fast photodetector [72] and the Agilent Infiniium DCA-J 86100C oscilloscope. The piezo voltage of the measurement system is used to adjust the phase difference between the input pulses ψ_{Int} to show full constructive and destructive interference of the centre pulse.

To assess the phase properties of the prototype device over a longer period of time, the probe signal generated by the measurement system is sent into the device and a constant voltage is applied to the on-chip AMZI heater element. The phase properties of the probe signal, ψ_{Int}, are calculated using the reference signal and combined with the phase calculated from the signal measured at D_P to extract the phase imparted by the prototype device, $\phi_{Rx.}$. Initially the heater voltage is set to 0 V and three sweeps of the measurement system piezo are performed, where the piezo voltage is varied between 0 V and 70 V in incremental steps of 0.1 V. This piezo sweep varies the phase of the probe signal, ψ_{Int}, and each full sweep of the piezo takes ~ 13.7 minutes. The heater voltage is then set to V_{max} and a piezo sweep is performed, where across the entire sweep the supply current from the temperature controller increases to counteract the heat dissipation from the heater. On the beginning of the second piezo sweep, the drive current from the temperature controller reaches the set threshold and the heater voltage is turned down to V_{16}. The supplied current from the temperature controller sharply decreases, but then begins to increase slowly and subsequently reaches the threshold during the following piezo sweep. The heater voltage is turned down to V_{15}, where the temperature controller is able to stabilise the temperature on-chip at a suitable supply current. The heater voltage is then left at setting V_{15} for 18 sweeps of the piezo voltage, taking ~ 4 hours 25 minutes. After which, the heater voltage is switched back to 0 V and four sweeps of the piezo are performed. The resulting variation in the calculated phase of the prototype receiver, $\Delta\phi_{Rx.}$, is shown in figure 5.15, where the shaded regions indicate the measurement uncertainty calculated using $\varepsilon_{Temp} = 0.1$ mrad and $\varepsilon_{\lambda} = 20$ mrad.

Enhanced plots of the first 3 sweeps at a heater setting of 0 V and the 18 sweeps performed at a heater setting of V_{15} are shown in figure 5.16. Some variation can be seen in $\Delta\phi_{Rx.}$ for the V_{15} setting over the measurement time. However, notably the measured phase appears very consistent from 380 minutes onwards. The weighted mean phase for the 0 V heater setting is $\Delta\psi_{Rx.} = 0.0086 \pm 0.0382$ and for the V_{15} setting is $\Delta\psi_{Rx.} = -0.607 \pm 0.035$, where the weightings are proportional to the inverse square of the measurement uncertainty.

5.3.2 Short Duration Assessment (Single-photon Level Signal)

For this measurement detectors D_{REF} and D_{MP} shown in figure 5.13 are power meters and detector D_P is the ID210 single-photon detector. The ID210 is operated at a clock rate of 40 MHz, set to have a detection efficiency of 25% and a dead time of 40 μs. The input power of the reference signal slow and fast polarisations are 1.2 nW and 0.50 nW respectively. The input power of the probe signal detected at D_{MP} is 8.9 pW, equivalent to 1.73 photons per pulse.

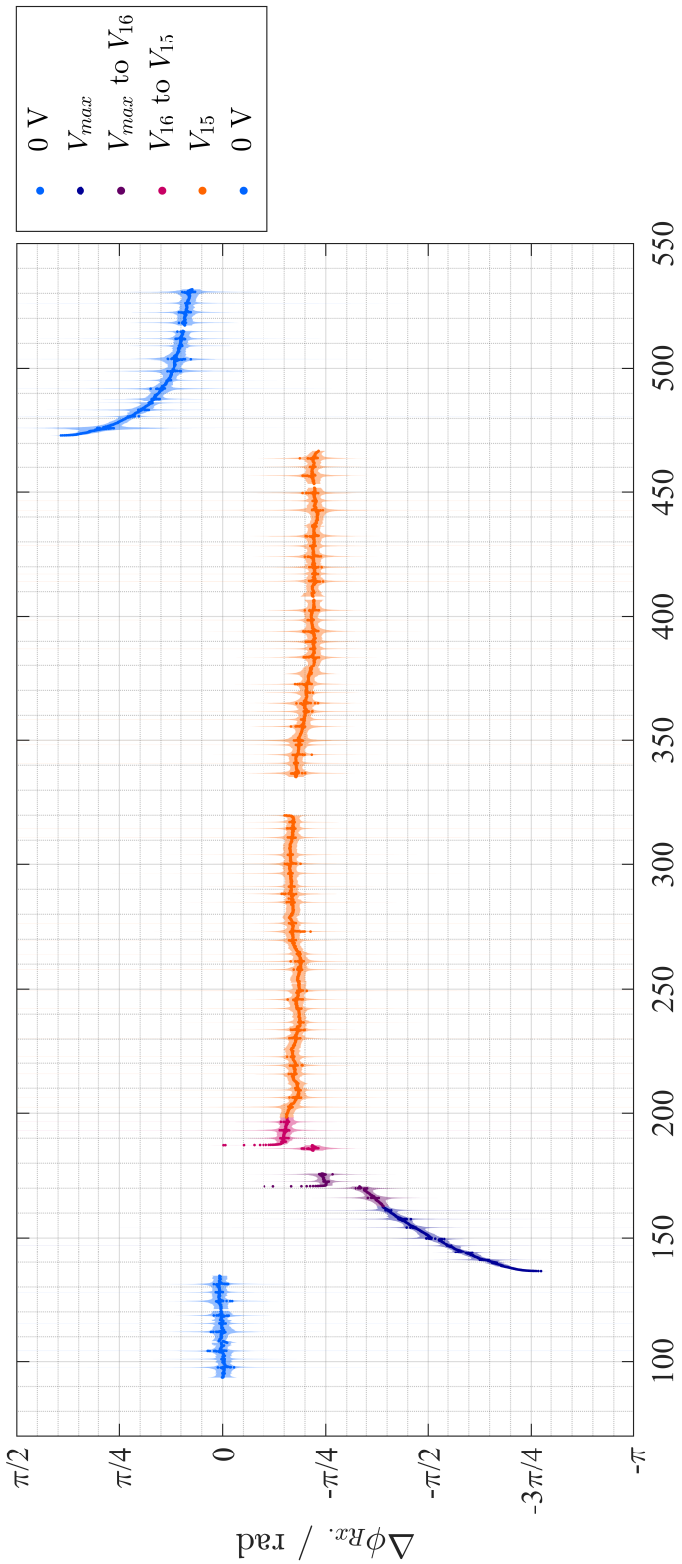


Figure 5.15: Measured variation in the phase of the prototype device AMZI $\Delta\phi_{Rx.}$ for various settings of the heater voltage. The shaded regions indicate the measurement uncertainty of the calculated phase. The heater voltages are applied in the same order as that shown in the legend. The heater voltage, initially switched from 0 V to V_{max}, is then switched down to V_{16} and then to V_{15} to allow the temperature controller to stabilise the temperature of the chip.

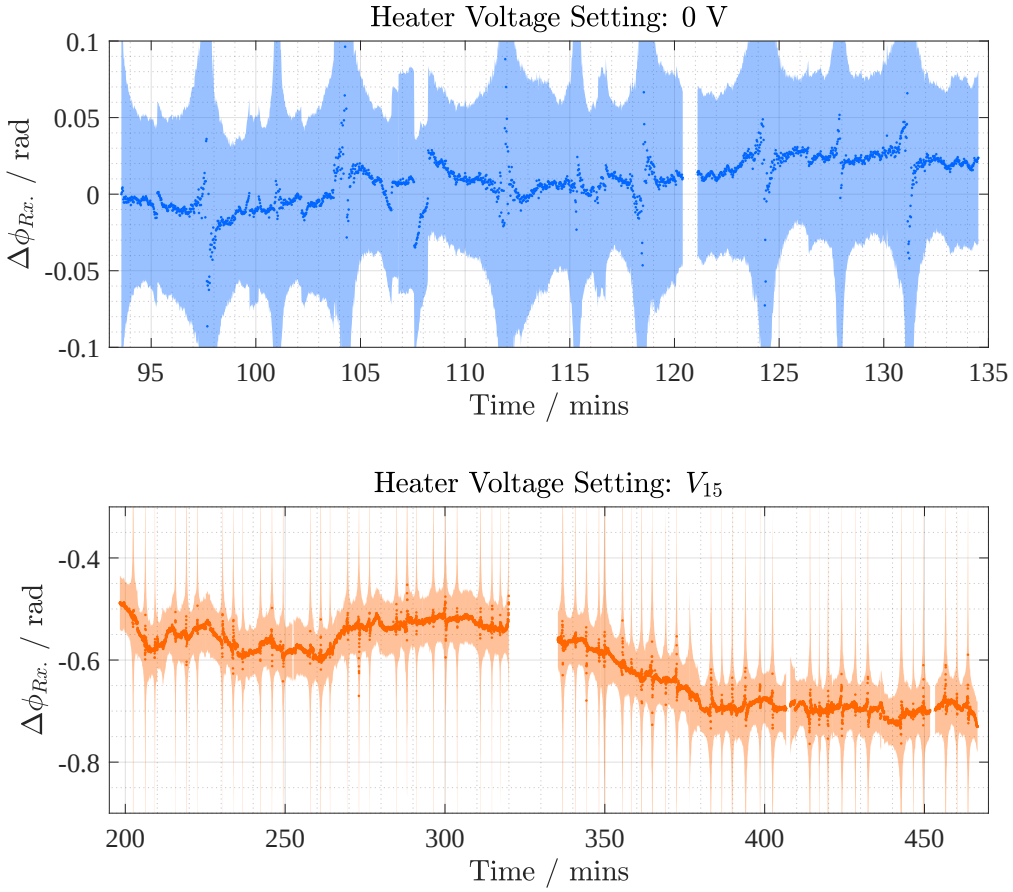


Figure 5.16: Measured variation in the phase of the prototype device AMZI $\Delta\phi_{Rx.}$ as shown in figure 5.15 for the 0 V and V_{15} heater settings. The shaded regions indicate the measurement uncertainty of the calculated phase. The 0 V heater settings are from the first three sweeps shown in figure 5.15.

In an ideal realisation of this experiment, a higher optical power would be sent to the monitoring power meter D_{MP} and a polarisation maintaining optical attenuator would be placed just before the QKD receiver to attenuate the probe signal to have a mean photon number per pulse ≤ 1, to avoid overloading the SPD's in the receiver. However, as this was not available for this experiment, the power of the probe signal was brought down as low as possible, so that the mean photon number per pulse was at the single-photon level, whilst still producing a detectable signal above the noise floor of the monitoring power meter D_{MP}. To accommodate this signal and avoid saturation of the single photon detector, a fixed optical attenuator is placed just before the input to the ID210. Figure 5.17 shows the number of counts detected at the ID210 when the heater voltage setting is 0 V and the piezo element in swept between 0 V and 70 V. Given the 40 µs dead time setting of the SPD, the maximum number of counts that can be recorded is 25 kHz. The resulting maximum and minimum detected mean photon number per pulse at the ID210 is 6.2×10^{-3} and 1.2×10^{-3} respectively. Temporarily the variable optical attenuator is used to increase the brightness of the probe signal, and traces of the interfering pulse pairs detected using the Thorlabs DXM30AF fast photodetector [72] and the Agilent Infiniium DCA-J 86100C oscilloscope at the receiver output are shown in figure 5.18. The piezo element of the measurement system is used to show full constructive and destructive interference of the centre pulse.

To assess the heater settings on a faster time scale, the measurement procedure involves alternating the voltage applied to the on-chip AMZI heater, whilst incrementally varying

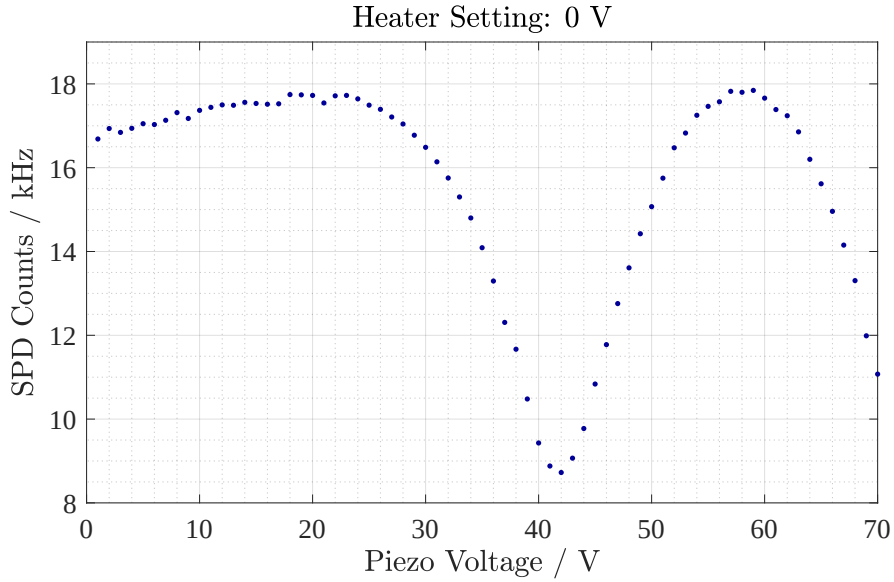


Figure 5.17: Counts detected by the ID210 SPD at the output of the prototype device in the setup shown in figure 5.13. The piezo element of the measurement system is varied between 0 V and 70 V producing an interference pattern, whilst the heater voltage setting of the on-chip AMZI is kept at 0 V.

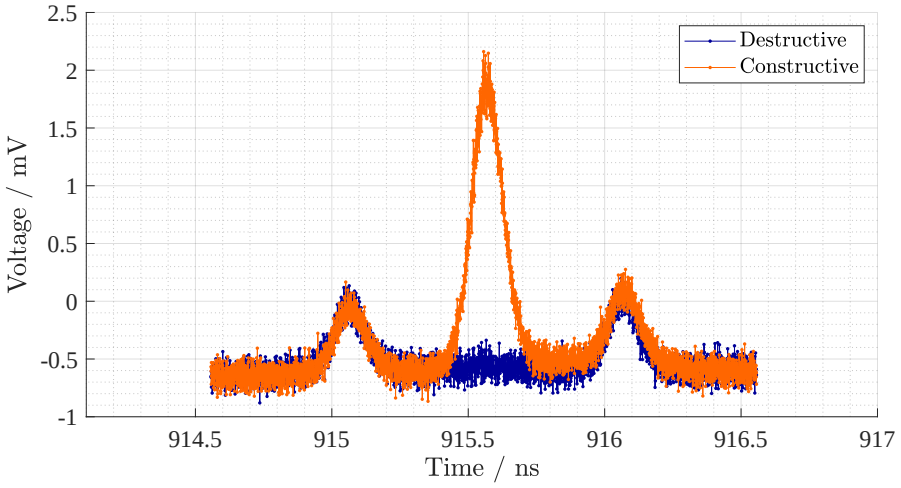


Figure 5.18: Traces of the interfering pulse pairs of the probe signal detected at the output of the prototype receiver. The piezo element of the measurement system is adjusted to show full constructive and destructive interference of the centre pulse.

the piezo voltage of the measurement system. The measurement proceeds as follows:

1. The piezo voltage is set to the starting voltage
2. The heater voltage is set to 0 V and 15 data points are recorded ($\sim$ 53 s)
3. The heater voltage is set to a non-zero voltage V_H and 15 data points are recorded ($\sim$ 53 s)
4. The piezo voltage is incremented and steps 2 - 3 are repeated until the final piezo voltage setting is reached

The piezo voltage is swept between 0 V and 70 V in incremental steps of 1 V and each sweep, following the procedure above, takes $\sim$ 60 minutes. Figure 5.19 shows the power ratio of the probe signal, the mean photon number per pulse detected at D_P divided by the optical power detected at D_{MP}, resulting from the measurement procedure described. The data shown results from five switches of the heater voltage between 0 V and V_{max}, where after each set of 30 data points (15 points for the 0 V setting and 15 points for the V_{max} setting), the piezo voltage is incremented. When switching the heater voltage, there is delay of $\sim$ 5 s between the control software commanding the voltage change to the on-chip AMZI heater and the voltage actually being applied. After this point the power ratio changes dramatically, and appears to roughly stabilise by the final (15^{th}) data point. To compare the heater voltage settings, the the 15^{th} data point of each data set is used to calculate the receiver phase $\phi_{Rx.}$.

The measurement procedure is repeated five times for the non-zero heater voltage settings of V_{max}, V_{16}, V_{12}, V_8 and V_4, resulting in five sweeps of the piezo element. Figure 5.20 shows plots of the power ratio from every 15^{th} data point for each of the voltage settings applied to the heater. These power ratios are then used to calculate the value of $\Delta\phi_{Rx.}$, which are shown in figure 5.21. The shaded regions in the figure indicate the measurement uncertainty, where $\varepsilon_{Temp} = 0.1$ mrad and $\varepsilon_{\lambda} = 20$ mrad. Some drift in the receiver phase can be seen for the setting V_{max}, however the calculated phase for the other heater voltage settings appears consistent over the sweep. The weighted mean of each of the data sets and their associated uncertainties are detailed in table 5.4, where the weightings are proportional to the inverse square of the measurement uncertainty. This measurement procedure has resulted in a larger shift in the phase produced by the on-chip AMZI in the prototype device when compared to the experiments described previously in this chapter.

5.4 Prototype Assessment Summary

This chapter explores the assessment of a prototype QKD device using the measurement system, detailing the experimental setups and the results of the phase measurements performed. Two forms of assessment were carried out. The first combined the prototype component with a laser source to generate a QKD signal, that was then assessed using the measurement system combined with detectors; demonstrating the application of the measurement system to the characterisation of QKD transmitter modules. The second formulation combined the measurement system with a laser source to generate a probe signal, that was then sent into the prototype component combined with a detector to measure the phase properties of the on-chip AMZI. This demonstrates the application of the measurement system to the characterisation of QKD receiver modules. Further discussion of the results are detailed in chapter 6.

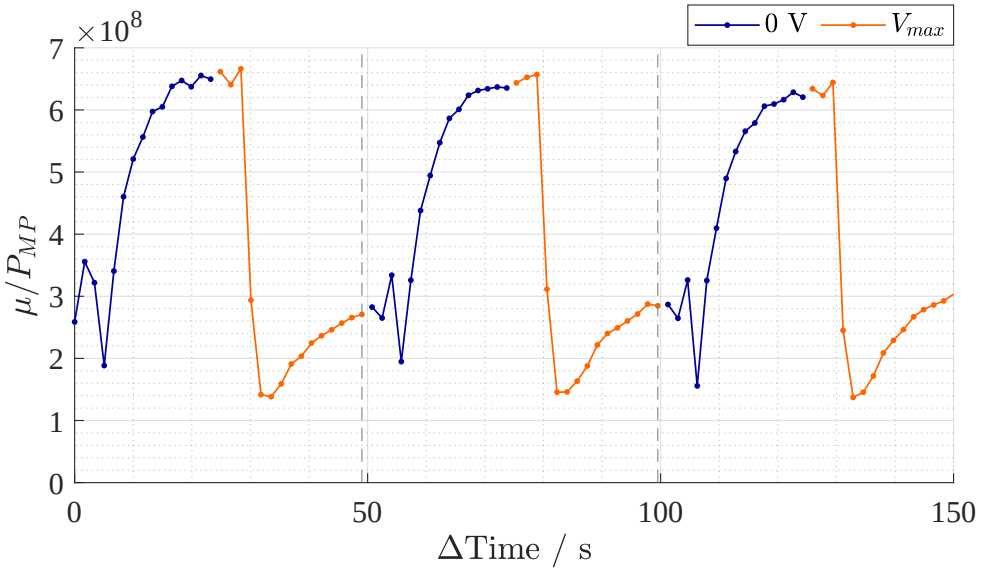


Figure 5.19: Detected power ratio of the probe signal for five switches of the heater voltage setting between 0 V and V_{max}. Each data set corresponding to a heater voltage setting consists of 15 data points. The dashed vertical lines represent the point just prior to the piezo voltage being incremented.

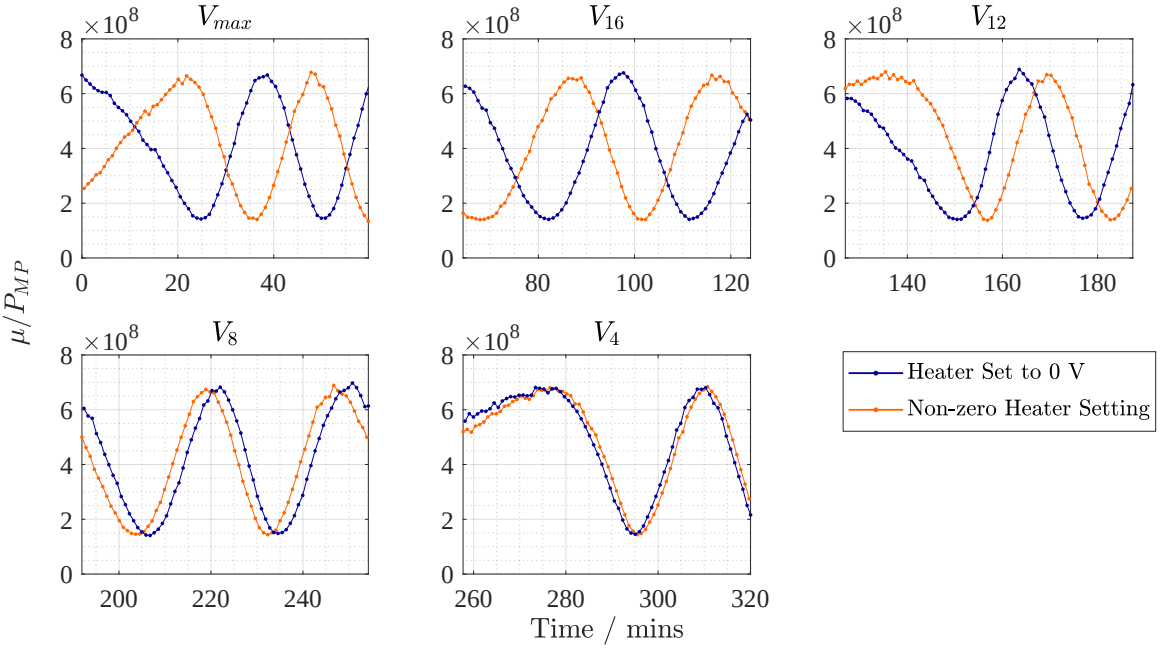


Figure 5.20: Plots of every 15$^{\text{th}}$ data point of the recorded power ratio of the probe signal across the piezo sweeps. Each subplot shows two interference patterns, one for a heater setting of 0 V and the other for a non-zero heater setting, as specified in the plot title. The offset of the interference patterns between the 0 V and non-zero heater setting indicates the size of the applied phase shift.

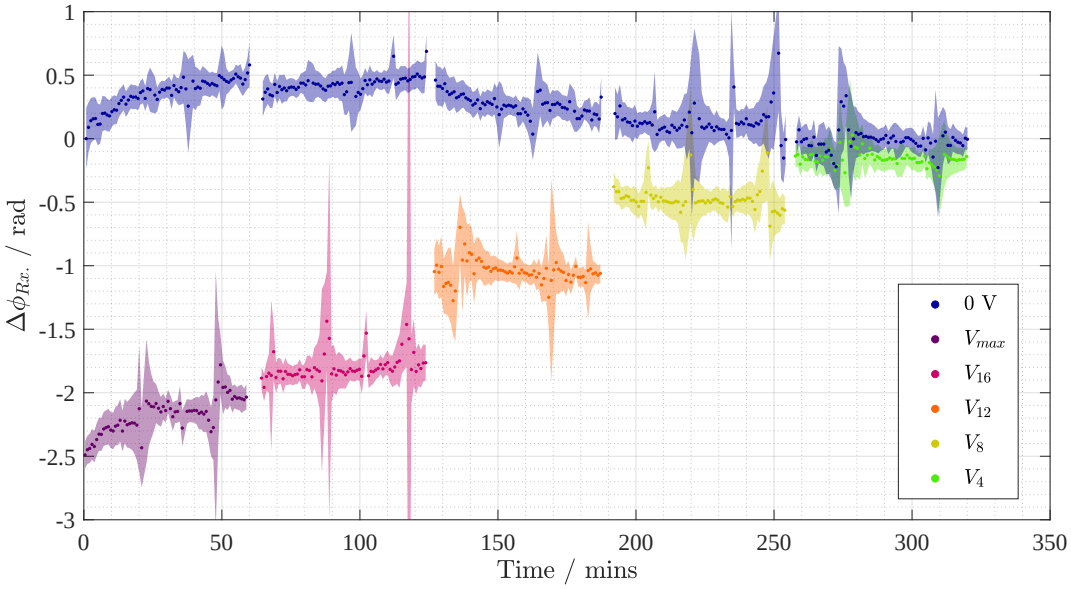


Figure 5.21: Calculated $\Delta\phi_{Rx.}$ over time for the fast measurement procedure. Five sweeps of the piezo voltage are performed, corresponding to the non-zero heater voltage settings V_{max}, V_{16}, V_{12}, V_8 and V_4. The shaded regions indicate the measurement uncertainty of the phase value.

Non-zero Heater Setting	**Heater Setting: 0 V** $\Delta\phi_{Rx.}$ **/ rad**	**Non-zero Heater Setting** $\Delta\phi_{Rx.}$ **/ rad**
V_{max}	0.375 ± 0.102	-2.170 ± 0.122
V_{16}	0.430 ± 0.096	-1.828 ± 0.105
V_{12}	0.259 ± 0.104	-1.055 ± 0.102
V_8	0.106 ± 0.125	-0.484 ± 0.110
V_4	-0.017 ± 0.110	-0.159 ± 0.104

Table 5.4: Weighted mean values of $\Delta\phi_{Rx.}$ shown in figure 5.21 and their corresponding uncertainties for various settings of the heater voltage.

Chapter 6

Conclusions

This thesis reports the design, construction and initial experimental implementation of a measurement system for characterising the phase properties of quantum key distribution (QKD) devices. The measurement system is designed such that it can be combined with single-photon detectors (SPD) to characterise the single-photon level signal produce by a QKD transmitter. Alternatively, it can be combined with a laser source to generate a probe signal of known phase properties, which can be used to characterise a QKD receiver. The measurement system is plug-and-play by design, simplifying the experimental setup for the characterisation measurement of a QKD device and allowing the system to be easily applied to any QKD module. The system is also portable, so that it can be used to characterise devices in situ as part of an integrated QKD system or network.

The theoretical model of the measurement system covers the main functionality of the internal optics and provides predictions for contributions to the final phase measurement uncertainty, resulting from limitations in the measurement system and uncontrollable fluctuations in the surrounding environment. The model aided the design of the measurement system; the most notable instance of this is the use of two polarisation states of the reference signal to reduce the measurement uncertainty of the final result. The model could be expanded to include the polarisation state in the mode of the coherent states representing the laser signals. This would require the inclusion of four-mode beam splitters (two spatial modes and two polarisation modes) [47] and would allow features such as polarisation crosstalk to be included. Note that, in the work completed in this project, the two polarisation states of the reference signal were purposefully sent alternately to avoid significant issues relating to polarisation cross talk. If the measurement system was ever implemented with a sufficiently long fibre optical path difference (OPD), it may also be necessary to consider the effects of Raman and Rayleigh scattering [81] in the model.

The characterisation test procedures developed here focus on the post-processing of data to provide the best phase measurement accuracy and the most reasonable measurement uncertainty. Elements of these test procedures have been implemented into the LabVIEW software program that controls the operation of the hardware components of the measurement system and records all of the data required for the phase analysis. Functionality involving the real-time processing of phase calculations has been developed and the necessary calibration steps for this have been detailed. Further work can be done to develop real-time processing analysis techniques and the implementation of this in the system control software. This would be particularly useful when performing measurements in situ, where the time available for the experiment may be limited.

In this work, the test procedures used have focussed on measuring the change in the interferometer phase, $\Delta\theta_{IntR}$ and $\Delta\theta_{IntQ}$, such that the final calculated phase values describe the phase change in the QKD or probe signal, $\Delta\phi_Q$. This is due to the phase conversion technique between the reference and QKD/probe signal, where method 2 detailed

in section 2.4.2 is implemented. In future work, characterisation measurements following method 1 (section 2.4.2) should be carried out, incorporating the additional calibration step required to determine the value of the QKD signal phase, ϕ_Q.

The functionality of the measurement system was demonstrated in chapters 3 and 4, including the performance of the software-based PID loop for locking the interferometer phase against varying lengths of OPD, and the assessment of continuous wave and pulsed laser sources. Work was also done to develop and test a pseudo QKD signal, generated using a pulsed laser and a phase modulator, performed with both bright and single-photon level signals. The results from these experiments demonstrate the functionality of the measurement system, highlighting the flexible application of the system to various measurements. This is particularly notable in the assessment of the pulsed laser signal, where the obvious lack of an interference pattern and the estimation of the values of the power ratio maximum and minimum established the incoherence between the individual pulses produced by the laser. Further work to develop this type of measurement, potentially with the inclusion of tagged pulses and randomness tests, would allow for the assessment of the randomised global phase of QKD pulse trains required by certain protocols, for example phase-encoded BB84. In addition to this, further work to characterise the measurement system could be completed against stabilised and traceable optical sources, providing a more thorough assessment of the measurement system itself.

The fifth chapter focussed on the assessment of a prototype chip-based QKD component, where two experimental setups were used to investigate its performance. One of the experimental setups combined the prototype device with a pulsed laser source to generate a QKD signal that could be assessed by the measurement system, demonstrating the application of the system to the characterisation of QKD transmitter modules. The second experimental setup involved combining the prototype device with a single-photon detector and using a pulsed laser with the measurement system to generate a probe signal to send into the prototype, demonstrating the application of the measurement system to the characterisation of a QKD receiver module. The execution of these experiments predominantly focussed on long-term measurements of the phase of the prototype device, resulting in the continuous application of voltage to the on-chip heating element for extended periods. This is not necessarily the mode of operation this prototype component is best suited for, so some of the resulting features would not necessarily be present in the real-world application of this device.

The results from the prototype device assessment showed clear phase modulation performed by the component in both the transmitter and receiver assessment experimental formulations, using bright and single-photon level QKD/probe signals. The largest phase response was seen for the faster switching of the heater voltage, where the heater setting was changed between 0 V to a non-zero voltage every ~ 53 s. The resulting phase values were far more consistent over the sweep of the measurement system's piezo element and the maximum change in the measured phase for the application of V_{max} to the heater is $\Delta\phi_{Rx.} = 2.55 \pm 0.22$ rad. In all of the resulting data sets some drift in the calculated phase was seen, which has been attributed to the thermal stabilisation of the chip, where the variation in the device's temperature would effect the OPD of the on-chip AMZI and the imparted phase ϕ_Q (or $\phi_{Rx.}$). Further investigation into the temperature control of the device, including the operation of the Thorlabs TED200C temperature controller, should be completed. In addition to this, experiments involving the time-tagging of individual pulses would enable an analysis of the component performance when modulated on faster timescales. This was not possible within the timescale of this project, requiring the development of electronics able to deliver the requisite pulses to drive the heater. While thermo-optic phase modulating devices (the heater) are typically limited to the kHz timescales, other approaches can generate modulation rates in the GHz regime [38, 82,

83].

This project is aimed to enhance the National Physical Laboratory's ability to evaluate the implementation security of prototype or commercial QKD systems, where the work reported here forms an initial step towards developing the capability for phase characterisation measurements of QKD modules. Future work to further develop this capability could involve the use of traceable highly wavelength-stabilised reference lasers, to reduce the measurement uncertainty in the calculated phase values, as well as the use of lock-in techniques for improved stabilisation.

Appendix A

Appendices for Chapter 1

A.1 Quantum Mathematical Definitions

The qubit states used in the phase-encoded BB84 protocol [17] are eigenstates of the Pauli matrices. The qubit states are defined as,

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$|+\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \qquad |-\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

and the three Pauli matrices are defined as,

$$\hat{\sigma}_X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \hat{\sigma}_Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad \hat{\sigma}_Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Only the bases defined by the $\hat{\sigma}_Z$ and $\hat{\sigma}_X$ Pauli matrices are used in the BB84 protocol. The qubit states $|0\rangle$ and $|1\rangle$ are eigenstates of the $\hat{\sigma}_Z$ Pauli matrix (Z-basis) and the qubit states $|+\rangle$ and $|-\rangle$ are eigenstates of the $\hat{\sigma}_X$ Pauli matrix (X-basis), such that,

$$\hat{\sigma}_Z |0\rangle = |0\rangle \qquad \hat{\sigma}_Z |1\rangle = -|1\rangle$$
$$\hat{\sigma}_X |+\rangle = |+\rangle \qquad \hat{\sigma}_X |-\rangle = -|-\rangle.$$

The diagonal qubit states, $|+\rangle$ and $|-\rangle$, can be written as a superposition of $|0\rangle$ and $|1\rangle$ as follows,

$$|+\rangle = \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \qquad \text{(1.1, revisited)}$$

$$|-\rangle = \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \qquad \text{(1.2, revisited)}$$

where similar expressions for $|0\rangle$ and $|1\rangle$ in terms of $|+\rangle$ and $|-\rangle$ can also be written,

$$|0\rangle = \frac{1}{\sqrt{2}} (|+\rangle + |-\rangle) \qquad \text{(1.3, revisited)}$$

$$|1\rangle = \frac{1}{\sqrt{2}} (|+\rangle - |-\rangle). \qquad \text{(1.4, revisited)}$$

A useful summary regarding these definitions and notation can be found in [84].

Appendix B

Appendices for Chapter 2

B.1 Gaussian Pulsed Laser Light

B.1.1 Laser Pulse Definition

It is assumed that the laser pulses have a Gaussian temporal distribution. A Gaussian probability distribution is generally defined as,

$$P\left(x\right) = \frac{1}{\sigma\sqrt{2\pi}} e^{(x-\mu)^2/2\sigma^2}$$

where P is the probability density as a function of variable x, σ is the standard deviation of the distribution and μ is the mean value of x. The full width half maximum of the distribution is given by $2\sqrt{2\ln(2)}$. For a laser pulse k, the variable is time ($x = t$), the mean time is set to $\mu = \delta_k$ (the centre point of pulse k), and the full width half maximum is denoted by $\tau_k = 2\sqrt{2\ln(2)}$. Substituting these values into the above equation results in,

$$P(t) = G_k^2 = \left(\frac{4\ln(2)}{\pi\tau_k^2}\right)^{\frac{1}{2}} e^{-4\ln(2)(t-\delta_k)^2/\tau_k^2}$$

the Gaussian distribution of a single optical pulse k. The coherent state representing laser pulse k can therefore be written as [47],

$$|G_k\alpha_k\rangle = e^{-\frac{{G_k}^2|\alpha_k|^2}{2}} \sum_{n=0}^{\infty} \frac{\left(G_k\alpha_k\right)^n}{\sqrt{n!}} |n\rangle \qquad \text{(2.5 revisited)}$$

where,

$$G_k = \left(\frac{4\ln(2)}{\pi\tau_k^2}\right)^{\frac{1}{4}} e^{-2\ln(2)(t-\delta_k)^2/\tau_k^2}. \qquad \text{(2.6 revisited)}$$

B.1.2 Mean Photon Number per Pulse

The mean photon number of laser light pulse k is given by [47],

$$\mu_k = \int_{-\infty}^{\infty} \left| G_k\alpha_k e^{i\phi_k} \right|^2 dt$$

where substitution of the expression for G_k (equation 2.6) results in,

$$\begin{aligned}\mu_k &= |\alpha_k|^2 \int_{-\infty}^{\infty} G_k^2 dt \\ &= |\alpha_k|^2 \left(\frac{4\ln(2)}{\pi\tau_k^2}\right)^{\frac{1}{2}} \int_{-\infty}^{\infty} e^{-4\ln(2)t_k^2/\tau_k^2} dt.\end{aligned}$$

Substituting in $u = 2\sqrt{\ln(2)}\frac{t-\delta_k}{\tau_k}$, where $\frac{du}{dt} = 2\sqrt{\ln(2)}\frac{1}{\tau_k}$, gives,

$$\begin{aligned}\mu_k &= |\alpha_k|^2 \left(\frac{4\ln(2)}{\pi\tau_k^2}\right)^{\frac{1}{2}} \int_{-\infty}^{\infty} e^{-u^2} \frac{\tau_k}{2\sqrt{\ln(2)}} du \\ &= |\alpha_k|^2 \frac{1}{\sqrt{\pi}} \int_{-\infty}^{\infty} e^{-u^2} du \\ &= |\alpha_k|^2\end{aligned}$$

Therefore the mean photon number of a laser pulse k with a Gaussian temporal distribution is given by,

$$\mu_k = \int_{-\infty}^{\infty} \left| G_k \alpha_k e^{i\phi_k} \right|^2 dt = |\alpha_k|^2 . \qquad \text{(2.7 revisited)}$$

B.2 Interferometer Model

B.2.1 Attenuation Operation

The attenuation operation can be derived from the partial trace of the two-spatial-mode beamsplitter, whose operation is defined by [46, 47],

$$\hat{B}_{2l} |\alpha\rangle_a |\beta\rangle_b = |\sqrt{T_l}\alpha - i\sqrt{R_l}e^{i\psi_{Bl}}\beta\rangle_{a'} |\sqrt{T_l}\beta - i\sqrt{R_l}e^{-i\psi_{Bl}}\alpha\rangle_{b'} . \qquad \text{(2.11 revisited)}$$

For an input state of $|\alpha\rangle_a |0\rangle_b$ into the beamsplitter, the resulting state can be written as,

$$\begin{aligned}\hat{B}_{2l} |\alpha\rangle_a |0\rangle_b &= |\sqrt{T_l}\alpha\rangle_{a'} |-i\sqrt{R_l}e^{-i\psi_{Bl}}\alpha\rangle_{b'} \\ &= |\gamma\rangle_{a'} |\nu\rangle_{b'}\end{aligned}$$

where $\gamma = \sqrt{T_l}\alpha$ and $\nu = -i\sqrt{R_l}e^{-i\psi_{Bl}}\alpha$. The density matrix of this output state is given by,

$$\begin{aligned}\rho_{a'b'} &= |\gamma\rangle\langle\gamma|_{a'} \otimes |\nu\rangle\langle\nu|_{b'} \\ &= |\gamma\rangle\langle\gamma|_{a'} \otimes e^{-|\nu|^2} \sum_{n,m=0}^{\infty} \frac{\nu^n (\nu^*)^m}{\sqrt{n!m!}} |n\rangle\langle m|_{b'}\end{aligned}$$

where taking the partial trace of this with respect to the b' mode results in,

$$\begin{aligned}tr_{b'}(\rho_{a'b'}) &= |\gamma\rangle\langle\gamma|_{a'} e^{-|\nu|^2} \sum_{n,m=0}^{\infty} \frac{\nu^n (\nu^*)^m}{\sqrt{n!m!}} \langle m|n\rangle \\ &= |\gamma\rangle\langle\gamma|_{a'} e^{-|\nu|^2} \sum_{n=0}^{\infty} \frac{\left(|\nu|^2\right)^n}{n!} \\ &= |\gamma\rangle\langle\gamma|_{a'} .\end{aligned}$$

Therefore we can model attenuation of the optical signal as a partial trace of the beamsplitter operation [47],

$$\begin{aligned}\hat{A}_a |\alpha\rangle_a &= tr_{b'}\left(\hat{B}_{2l}\hat{B}_{2l}^{\dagger}\left[|\alpha\rangle\langle\alpha|_a \otimes |0\rangle\langle 0|_b\right]\right) \\ &= |\sqrt{T_l}\alpha\rangle_{a'}\end{aligned}$$

which, on reverting the spatial mode from a' back to a, is simplified to the stated attenuation operator,

$$\hat{A}_{jl} |\alpha\rangle_j = |\sqrt{\eta_{jl}}\alpha\rangle_j \qquad \text{(2.12, revisited)}$$

where $T_l = \eta_{jl}$ the transmittance for spatial mode j and attenuator l.

B.2.2 Evolution of the Quantum State

Equations for the optical power detected are derived when measuring pulses k and $k+1$ in the interferometer model; see figure 2.4. The operators used in the model are restated below [46, 47],

Beamsplitter:

$$\hat{B}_{2l}\left|\alpha\right\rangle_a\left|\beta\right\rangle_b = \left|\sqrt{T_l}\alpha - i\sqrt{R_l}e^{i\psi_{Bl}}\beta\right\rangle_{a'}\left|\sqrt{T_l}\beta - i\sqrt{R_l}e^{-i\psi_{Bl}}\alpha\right\rangle_{b'} \qquad \text{(2.11 revisited)}$$

Attenuation:

$$\hat{A}_{jl}\left|\alpha\right\rangle_j = \left|\sqrt{\eta_{jl}}\alpha\right\rangle_j \qquad \text{(2.12 revisited)}$$

Phase Shift:

$$\hat{P}_{jl}\left|\alpha\right\rangle_j = \left|e^{-i\psi_{jl}}\alpha\right\rangle_j \qquad \text{(2.13 revisited)}$$

where j is the spatial mode and l is the distinguishing index. For a single pulse k output from the QKD transmitter, represented by coherent state $|G_k\alpha_k e^{i\phi_k}\rangle$, the state evolves as follows,

$$\begin{aligned} \text{Input} \quad & \left|G_k\alpha_k e^{i\phi_k}\right\rangle_{a_0}\left|0\right\rangle_{b_0} \\ \hat{B}_{20} \;\rightarrow\; & \left|\sqrt{T_0}G_k\alpha_k e^{i\phi_k}\right\rangle_{a_0'}\left|-i\sqrt{R_0}e^{i\psi_{B0}}G_k\alpha_k e^{i\phi_k}\right\rangle_{b_0'} \end{aligned}$$

where the a_0' mode propagates to the AMZI and the b_0' mode is detected at detector $\mathrm{D_M}$. Following the b_0' mode, the optical power detected at $\mathrm{D_M}$ is given by,

$$\begin{aligned} P_M &= \eta_M \int_{-\infty}^{\infty} \left|-i\sqrt{R_0}e^{i\psi_{B0}}G_k\alpha_k e^{i\phi_k}\right|^2 dt \\ &= \eta_M R_0|\alpha_k|^2 \int_{-\infty}^{\infty} G_k^2\, dt \\ &= \eta_M R_0|\alpha_k|^2 \end{aligned} \qquad \text{(2.16, revisited)}$$

where η_M is the detection efficiency of detector $\mathrm{D_M}$. Alternatively, following the a_0' mode, the AMZI operates as follows,

$$\begin{aligned} \text{Input} \quad & \left|\sqrt{T_0}G_k\alpha_k e^{i\phi_k}\right\rangle_{a_0'}\left|0\right\rangle_{b_0'} \\ \hat{B}_{21} \;\rightarrow\; & \left|\sqrt{T_0T_1}G_k\alpha_k e^{i\phi_k}\right\rangle_a\left|-i\sqrt{T_0R_1}G_k\alpha_k e^{i(\phi_k-\psi_{B1})}\right\rangle_b \\ \hat{P}_a\hat{P}_b \;\rightarrow\; & \left|\sqrt{T_0T_1}G_k\alpha_k e^{i(\phi_k-\psi_a)}\right\rangle_a\left|-i\sqrt{T_0R_1}G_k\alpha_k e^{i(\phi_k-\psi_b-\psi_{B1})}\right\rangle_b \\ \hat{A}_a\hat{A}_b \;\rightarrow\; & \left|\sqrt{\eta_aT_0T_1}G_k\alpha_k e^{i(\phi_k-\psi_a)}\right\rangle_a\left|-i\sqrt{\eta_bT_0R_1}G_k\alpha_k e^{i(\phi_k-\psi_b-\psi_{B1})}\right\rangle_b. \end{aligned}$$

Before the final beamsplitter $\hat{B}_{22}$, the quantum state must incorporate the temporal delay experienced by the light propagating in each arm of the AMZI. The temporal delay imparted by AMZI arm j, denoted δ_j, can therefore be incorporated via the Gaussian function as follows [47],

$$G_k(t) \rightarrow G_k\left(t-\delta_j\right) = G_{kj} = \left(\frac{4\ln(2)}{\pi\tau_k^2}\right)^{\frac{1}{4}} e^{-2\ln(2)(t-\delta_k-\delta_j)^2/\tau_k^2}.$$

Therefore the optical state just before $\hat{B}_{22}$ is given by,

$$\text{Delay} \quad \left|\sqrt{\eta_aT_0T_1}G_{ka}\alpha_k e^{i(\phi_k-\psi_a)}\right\rangle_a\left|-i\sqrt{\eta_bT_0R_1}G_{kb}\alpha_k e^{i(\phi_k-\psi_b-\psi_{B1})}\right\rangle_b.$$

For the successful overlap and therefore interference of pulses k and $k+1$, then the k pulse must travel through path b and pulse $k+1$ must travel through path a. Assuming

successful overlap, the output optical state for the centre pulse from the AMZI (the pulse resulting from the overlap of k and $k+1$) is derived as follows,

$$\begin{aligned}\text{Input} \quad & |\sqrt{\eta_a T_0 T_1} G_{(k+1)a} \alpha_{k+1} e^{i(\phi_{k+1}-\psi_a)}\rangle_a \, |-i\sqrt{\eta_b T_0 R_1} G_{kb} \alpha_k e^{i(\phi_k-\psi_b-\psi_{B1})}\rangle_b \\ \hat{B}_{22} \rightarrow \; & |\sqrt{\eta_a T_0 T_1 T_2} G_{(k+1)a} \alpha_{k+1} e^{i(\phi_{k+1}-\psi_a)} - \sqrt{\eta_b T_0 R_1 R_2} G_{kb} \alpha_k e^{i(\phi_k-\psi_b-\psi_{B1}+\psi_{B2})}\rangle_{a'} \\ & |-i\sqrt{\eta_b T_0 T_2 R_1} G_{kb} \alpha_k e^{i(\phi_k-\psi_b-\psi_{B1})} - i\sqrt{\eta_a T_0 T_1 R_2} G_{(k+1)a} \alpha_{k+1} e^{i(\phi_{k+1}-\psi_a-\psi_{B2})}\rangle_{b'} .\end{aligned}$$

The state is then detected at detectors D_1 and D_2.

B.2.3 Optical Power Detected

To simplify the following expressions for detected power, it is assumed that $\alpha_k = \alpha_{k+1}$. This is applicable for single-photon level QKD pulses as the mean photon number is considered to be consistent across all pulses. For certain protocols there may exist decoy states that have a different mean photon number compared to the encoding pulses; in this case the decoy states should be sifted from the data. The assumption also applies when using CW light as fluctuation in optical input power or phase over the AMZI asymmetry delay time is negligible.

The successful measurement of pulses k and $k+1$ equates to the overlap and interference of the portion of pulse k that travels down arm b and the portion of pulse $k+1$ that travels down arm a. The a' mode propagates towards detector D_1, where the detected power is given by,

$$\begin{aligned}P_1 &= \eta_1 \int_{-\infty}^{\infty} \Big| \sqrt{\eta_a T_0 T_1 T_2} G_{(k+1)a} \alpha_k e^{i(\phi_{k+1}-\psi_a)} \\ &\qquad - \sqrt{\eta_b T_0 R_1 R_2} G_{kb} \alpha_k e^{i(\phi_k-\psi_b-\psi_{B1}+\psi_{B2})} \Big|^2 dt \\ &= \eta_1 T_0 |\alpha_k|^2 \int_{-\infty}^{\infty} \Big[\eta_a T_1 T_2 G_{(k+1)a}^2 + \eta_b R_1 R_2 G_{kb}^2 \\ &\qquad - 2\sqrt{\eta_a \eta_b T_1 T_2 R_1 R_2} G_{(k+1)a} G_{kb} \cos\left(\phi_{k+1} - \phi_k - \psi_a + \psi_b + \psi_{B1} - \psi_{B2}\right) \Big] dt \\ &= \eta_1 T_0 |\alpha_k|^2 \Big[\eta_a T_1 T_2 + \eta_b R_1 R_2 \\ &\qquad - 2\sqrt{\eta_a \eta_b T_1 T_2 R_1 R_2} \cos\left(\phi_Q + \psi_{Int}\right) \int_{-\infty}^{\infty} G_{(k+1)a} G_{kb} \, dt \Big] \end{aligned} \tag{B.1}$$

and where $\phi_Q = \phi_{k+1} - \phi_k$ and $\psi_{Int} = \psi_b - \psi_a + \psi_{B1} - \psi_{B2}$. A similar expression for the detection of mode b' at detector D_2 is given by,

$$\begin{aligned}P_2 &= \eta_2 \int_{-\infty}^{\infty} \Big| -i\sqrt{\eta_b T_0 T_2 R_1} G_{kb} \alpha_k e^{i(\phi_k-\psi_b-\psi_{B1})} \\ &\qquad - i\sqrt{\eta_a T_0 T_1 R_2} G_{(k+1)a} \alpha_{k+1} e^{i(\phi_{k+1}-\psi_a-\psi_{B2})} \Big|^2 dt \\ &= \eta_2 T_0 |\alpha_k|^2 \int_{-\infty}^{\infty} \Big[\eta_b T_2 R_1 G_{kb}^2 + \eta_a T_1 R_2 G_{(k+1)a}^2 \\ &\qquad + 2\sqrt{\eta_a \eta_b T_1 T_2 R_1 R_2} G_{(k+1)a} G_{kb} \cos\left(\phi_{k+1} - \phi_k - \psi_a + \psi_b + \psi_{B1} - \psi_{B2}\right) \Big] dt \\ &= \eta_2 T_0 |\alpha_k|^2 \Big[\eta_b T_2 R_1 + \eta_a T_1 R_2 \\ &\qquad + 2\sqrt{\eta_a \eta_b T_1 T_2 R_1 R_2} \cos\left(\phi_Q + \psi_{Int}\right) \int_{-\infty}^{\infty} G_{(k+1)a} G_{kb} dt \Big]. \end{aligned} \tag{B.2}$$

B.2.4 Power Expressions for Bright Light

If bright light is input into the AMZI and the monitoring photodiode D_M is used, then the power expressions B.1 and B.2 can be simplified to make them more suitable for the purposes of experimental analysis. Firstly, both P_1 and P_2 are divided by the monitor power P_M (equation 2.16), removing the effects of fluctuating input power.

$$\frac{P_1}{P_M} = \frac{\eta_1}{\eta_M}\frac{T_0}{R_0}\Big[\eta_a T_1 T_2 + \eta_b R_1 R_2 - 2\sqrt{\eta_a\eta_b T_1 T_2 R_1 R_2}\cos\left(\phi_Q + \psi_{Int}\right)\int_{-\infty}^{\infty} G_{(k+1)a} G_{kb}\, dt\Big]$$

$$\frac{P_2}{P_M} = \frac{\eta_2}{\eta_M}\frac{T_0}{R_0}\Big[\eta_b T_2 R_1 + \eta_a T_1 R_2 + 2\sqrt{\eta_a\eta_b T_1 T_2 R_1 R_2}\cos\left(\phi_Q + \psi_{Int}\right)\int_{-\infty}^{\infty} G_{(k+1)a} G_{kb} dt\Big].$$

For a sweep of the interferometer phase ψ_{Int}, the maximum and minimum values of the above expressions can be calculated. For D_1 these are,

$$\max\left(\frac{P_1}{P_M}\right) = \frac{\eta_1}{\eta_M}\frac{T_0}{R_0}\Big[\eta_a T_1 T_2 + \eta_b R_1 R_2 + 2\sqrt{\eta_a\eta_b T_1 T_2 R_1 R_2}\int_{-\infty}^{\infty} G_{(k+1)a} G_{kb}\, dt\Big]$$

$$\min\left(\frac{P_1}{P_M}\right) = \frac{\eta_1}{\eta_M}\frac{T_0}{R_0}\Big[\eta_a T_1 T_2 + \eta_b R_1 R_2 - 2\sqrt{\eta_a\eta_b T_1 T_2 R_1 R_2}\int_{-\infty}^{\infty} G_{(k+1)a} G_{kb}\, dt\Big].$$

The sum and difference of the maximum and minimum result in the following terms,

$$S_1 = \max\left(\frac{P_1}{P_M}\right) + \min\left(\frac{P_1}{P_M}\right) = 2\frac{\eta_1}{\eta_M}\frac{T_0}{R_0}\left(\eta_a T_1 T_2 + \eta_b R_1 R_2\right) \tag{B.3}$$

$$D_1 = \max\left(\frac{P_1}{P_M}\right) - \min\left(\frac{P_1}{P_M}\right) = 4\frac{\eta_1}{\eta_M}\frac{T_0}{R_0}\sqrt{\eta_a\eta_b T_1 T_2 R_1 R_2}\int_{-\infty}^{\infty} G_{(k+1)a} G_{kb}\, dt \tag{B.4}$$

where the same can be done for P_2/P_M. These terms can then be substituted back into the power ratio expressions resulting in,

$$\frac{P_1}{P_M} = \frac{1}{2}\left[S_1 - D_1\cos\left(\phi_Q + \psi_{Int}\right)\right] \tag{2.14, revisited}$$

$$\frac{P_2}{P_M} = \frac{1}{2}\left[S_2 + D_2\cos\left(\phi_Q + \psi_{Int}\right)\right] \tag{2.15, revisited}$$

where all of the non-phase parameters in these expressions can be measured and calculated during the experimental procedure.

B.2.5 Falling or Rising Factor χ

Equation 2.14 can be rearranged to give an expression for the phase of the output light,

$$\phi_Q + \psi_{Int} = \cos^{-1}\left(\frac{1}{D_1}\left[S_1 - 2\frac{P_1}{P_M}\right]\right) + \chi_1 \tag{2.22, revisited}$$

where the χ_1, termed the falling or rising factor, allows the phase to be unwrapped from the range of $[0, \pi]$ to $[0, 2\pi)$. The value of χ_1 will depend on the fringe gradient. As the value of $\phi_Q + \theta_{Int}$ varies from 0 to π, the output power detected at D_1 will increase, resulting in a rising edge. Whereas, when the value of $\phi_Q + \theta_{Int}$ varies from π to 2π, the

output power detected at D_1 will decrease, resulting in a falling edge. The value for χ_1 is therefore given by either,

$$\begin{aligned} &\text{Rising:} \quad \chi_1 = 0 \\ &\text{Falling} \quad \chi_1 = 2\pi - 2\cos^{-1}\left(\frac{1}{D_1}\left[S_1 - 2\frac{P_1}{P_M}\right]\right). \end{aligned}$$

Note that, given the fringe inversion between interferometer outputs, χ_2 for detector D_2 will incorporate terms D_2, P_2 etc. and the falling and rising equations will be swapped.

B.3 Phase Error due to Wavelength Instability

When using a reference laser to measure the phase difference of an interferometer, changes in the wavelength of the reference laser will create a perceived change in the interferometer phase. For convenience, the following equations from chapter 2 are restated,

$$OPD = OPL_a - OPL_b = \sum_m n_m L_{abm} \qquad \text{(2.28, revisited)}$$

$$\theta_{Int} = \frac{2\pi}{\lambda}\sum_m n_m L_{abm} \qquad \text{(2.30, revisited)}$$

where these can be combined to give the interferometer phase experienced by the reference signal,

$$\theta_{IntR} = \frac{2\pi}{\lambda_R} OPD_R.$$

If the wavelength of the reference laser changes from λ_R to λ'_R, the resulting change in the phase can be written as,

$$\begin{aligned} \Delta\theta_{IntR} &= \theta_{IntR} - \theta'_{IntR} \\ &= \frac{2\pi}{\lambda} OPD_{\lambda R} - \frac{2\pi}{\lambda'} OPD'_{\lambda R} \\ &= 2\pi\left(\frac{OPD_{\lambda R}}{\lambda_R} - \frac{OPD_{\lambda R} - \Delta OPD_{\lambda R}}{\lambda_R - \Delta\lambda_R}\right) \\ &= \frac{2\pi}{\lambda_R - \Delta\lambda_R}\left(\Delta OPD_{\lambda R} - \frac{\Delta\lambda_R}{\lambda_R} OPD_{\lambda R}\right) \end{aligned}$$

where $\Delta OPD_{\lambda R} = OPD_{\lambda R} - OPD'_{\lambda R}$ and $\Delta\lambda_R = \lambda_R - \lambda'_R$. Here a λ subscript is added to the OPD terms to indicate that the OPD has changed due to the wavelength change of the reference signal. From this, the change in phase experienced by the reference signal for a change in wavelength is given by,

$$\Delta\theta_{\lambda R} = \frac{2\pi}{\lambda_R - \Delta\lambda_R}\left(\Delta OPD_{\lambda R} - \frac{\Delta\lambda_R}{\lambda_R} OPD_{\lambda R}\right). \qquad \text{(2.61, revisited)}$$

B.4 Optical fibre Dispersion

B.4.1 Dispersion for Calculating the Temperature Error

Dispersion is the difference in time taken for two photons separated by 1 nm in wavelength, to traverse a distance of 1 km. To convert this into the variation in OPD between the QKD and reference signal, it is useful to consider the effect of dispersion in the two paths of the fibre interferometer as depicted in figure B.1. The time difference between the QKD

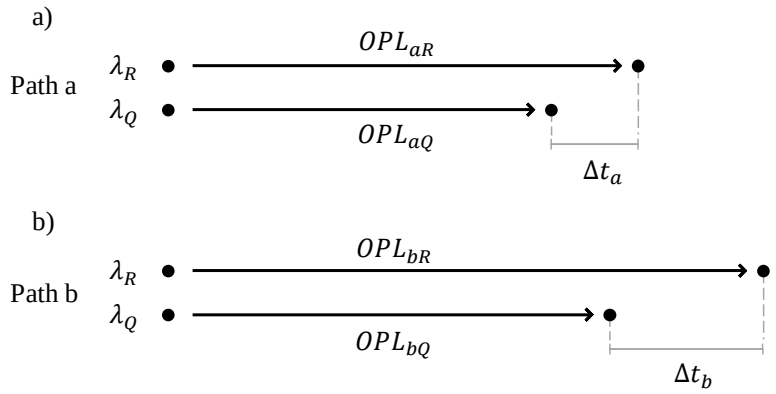


Figure B.1: Schematic of the effect of dispersion on the QKD and reference signal in the two paths, a and b, of a fibre AMZI. The time difference between the arriving photons for the QKD and reference signal in the two arms, Δt_a and Δt_b, is determined by the optical fibre dispersion, and can be equated to the variation in the OPD's of the two signals.

and reference signal in paths a and b, given by Δt_a and Δt_b respectively, can be equated to the variation in the OPD's between the two signals as follows,

$$\begin{aligned} n_R L_a - n_Q L_a &= OPL_{aR} - OPL_{aQ} = c\Delta t_a \\ n_R L_b - n_Q L_b &= OPL_{bR} - OPL_{bQ} = c\Delta t_b \end{aligned}$$

which can be combined to give,

$$\begin{aligned} OPL_{aR} - OPL_{aQ} - (OPL_{bR} - OPL_{bQ}) &= c\,(\Delta t_a - \Delta t_b) \\ OPD_{fibR} - OPD_{fibQ} &= c\,(L_a D\Delta\lambda - L_b D\Delta\lambda) \\ OPD_{fibR} - OPD_{fibQ} &= L_{ab\,fib} cD\Delta\lambda \qquad \text{(2.56, revisited)} \end{aligned}$$

where $OPD_{fibj} = OPL_{aj} - OPL_{bj}$ for $j = Q, R$, $\Delta t_a = L_a D\Delta\lambda$, $\Delta t_b = L_b D\Delta\lambda$ and $L_{ab\,fib} = L_a - L_b$. Differentiating this expression with respect to temperature results in,

$$\begin{aligned} \frac{d}{dT}\left(OPD_{fibR} - OPD_{fibQ}\right) &= \left(L_{ab\,fib}\frac{dD}{dT} + D\frac{dL_{ab\,fib}}{dT}\right) c\Delta\lambda \\ &= \left(\frac{dD}{dT} + D\alpha_{fib}\right) cL_{ab\,fib}\Delta\lambda \end{aligned}$$

where α_{fib} if the thermal expansion coefficient for the optical fibre. For a temperature change of ΔT, the difference between the OPD experienced by the QKD signal and the reference signal will change by,

$$\begin{aligned} \Delta OPD_{fibR} - \Delta OPD_{fibQ} &= \left(\frac{dD}{dT} + D\alpha_{fib}\right) cL_{ab\,fib}\Delta\lambda\Delta T \\ &\approx \frac{dD}{dT} cL_{ab\,fib}\Delta\lambda\Delta T \qquad \text{(2.58, revisited)} \end{aligned}$$

where in the final step the $D\alpha_{fib}$ is discounted as $O\left(D\alpha_{fib}\right) \sim 10^{-12}$ is much smaller than $O\left(dD/dT\right) \sim 10^{-9}$. Therefore the phase-wavelength error term can be written as,

$$\varepsilon_{Temp} = \frac{2\pi}{\lambda_Q}\left(\Delta OPD_{TempQ} - \Delta OPD_{TempR}\right) \qquad \text{(2.52, revisited)}$$

$$\varepsilon_{Temp\,fib} \approx \frac{2\pi}{\lambda_Q}\frac{dD}{dT} cL_{ab\,fib}\Delta\lambda\Delta T \qquad \text{(2.59, revisited)}$$

B.4.2 Dispersion for Calculating the Wavelength Error

Taking the following equation,

$$OPD_{fibR} - OPD_{fibQ} = L_{ab\,fib} cD\Delta\lambda \tag{2.56, revisited}$$

the OPD_{fibQ} term can be replaced by $OPD'_{\lambda R}$, the OPD experienced by the reference wavelength λ'_R. This results in the following equation,

$$\Delta OPD_{\lambda R} = L_{ab\,fib} cD\Delta\lambda_R \tag{2.65, revisited}$$

where $\Delta OPD_{\lambda R} = OPD_{\lambda R} - OPD'_{\lambda R}$. This can be combined with the following equations,

$$\varepsilon_\lambda = -\frac{\lambda_R}{\lambda_Q}\Delta\theta_{\lambda R} \tag{2.60, revisited}$$

$$\Delta\theta_{\lambda R} = \frac{2\pi}{\lambda_R - \Delta\lambda_R}\left(\Delta OPD_{\lambda R} - \frac{\Delta\lambda_R}{\lambda_R} OPD_{\lambda R}\right) \tag{2.61, revisited}$$

to derive an equation for the phase-wavelength error for fibre,

$$\begin{aligned}\varepsilon_{\lambda\,fib} &= -\frac{\lambda_R}{\lambda_Q}\frac{2\pi}{\lambda_R - \Delta\lambda_R}\left(\Delta OPD_{\lambda R} - \frac{\Delta\lambda_R}{\lambda_R} OPD_{\lambda R}\right) \\ &= -\frac{\lambda_R}{\lambda_Q}\frac{2\pi}{\lambda_R - \Delta\lambda_R}\left(cD - \frac{n_{fibR}}{\lambda_R}\right) L_{ab\,fib}\Delta\lambda_R.\end{aligned} \tag{2.66, revisited}$$

B.5 Minimum Perceivable Change in $\psi_{IntR\,[0,\pi]}$

For a small phase change $\Delta\psi_{IntR\,[0,\pi]} = \psi_{IntR\,[0,\pi]} - \psi'_{IntR\,[0,\pi]}$ within an AMZI, equation,

$$\psi_{IntR\,[0,\pi]} = \cos^{-1}\left(\frac{1}{D_{1R}}\left[S_{1R} - 2\frac{P_{1R}}{P_{MR}}\right]\right) \tag{2.38, revisited}$$

can be used to derive the following,

$$\begin{aligned}\cos(\psi_{IntR\,[0,\pi]}) - \cos(\psi'_{IntR\,[0,\pi]}) &= \frac{1}{D_{1R}}\left(S_{1R} - 2\frac{P_{1R}}{P_{MR}}\right) - \frac{1}{D_{1R}}\left(S_{1R} - 2\frac{P'_{1R}}{P_{MR}}\right) \\ &= -\frac{2}{D_{1R}}\frac{\Delta P_{1R}}{P_{MR}}\end{aligned}$$

where $\Delta P_{1R} = P_{1R} - P'_{1R}$ and it is assumed that S_{1R}, D_{1R} and P_{MR} are consistent across the phase change. This can be rearranged to give,

$$\Delta\psi_{IntR\,[0,\pi]} = \psi_{IntR\,[0,\pi]} - \cos^{-1}\left(\frac{2}{D_{1R}}\frac{\Delta P_{1R}}{P_{MR}} + \cos\left(\psi_{IntR\,[0,\pi]}\right)\right). \tag{2.67, revisited}$$

Appendix C

Appendices for Chapter 3

C.1 LabVIEW Software Control Screenshots

Event Handling Loop
[0] "Reinitialise": Value Change
[1] "Idle": Value Change
[2] "MDT694B Set Voltage": Value Change
[3] "Piezo Voltage Sweep": Value Change
[4] "Populate Heater Array": Value Change
[5] "Pz. Heater Sweep": Value Change
[6] "SRC-101 Control": Value Change
[7] "C-863.11 Control": Value Change
[8] "Switch Polarisation": Value Change
[9] "Set Polarisation": Value Change
[10] "Alternate Polarisations?": Value Change
[11] "Record Both": Value Change
[12] "Determine Edge Type": Value Change
[13] "Monitor Phase": Value Change
[14] "Min Max Sweep": Value Change
[15] "Set V/rad": Value Change
[16] "Lock to theta": Value Change
[17] "Lock to phi (0,pi)": Value Change
[18] "Refresh PID": Value Change
[19] "Unlock": Value Change
[20] "Read": Value Change
[21] "Refresh": Value Change
[22] "Clear Chart": Value Change
[23] "X-axis Range": Value Change
[24] "Save Now": Value Change
[25] "Stop": Value Change

Message Handling Loop
"Initialise"
"Idle", Default
"MDT694B Set"
"Piezo Voltage Sweep"
"Populate Heater Array"
"Piezo and Heater Sweep"
"SRC-101 Control"
"C-863.11 Control"
"Set Polarisation"
"Switch Polarisation"
"Alternate Polar."
"Record Both Polarisations"
"Determine Edge Type"
"Monitor Phase"
"Set V/rad"
"Min Max Sweep"
"Lock to Setpoint phi"
"Lock to Setpoint theta"
"Read"
"Refresh"
"Save"
"Stop"

Figure C.1: Screenshot of the event handling loop list and message handling loop list of the main LabVIEW program.

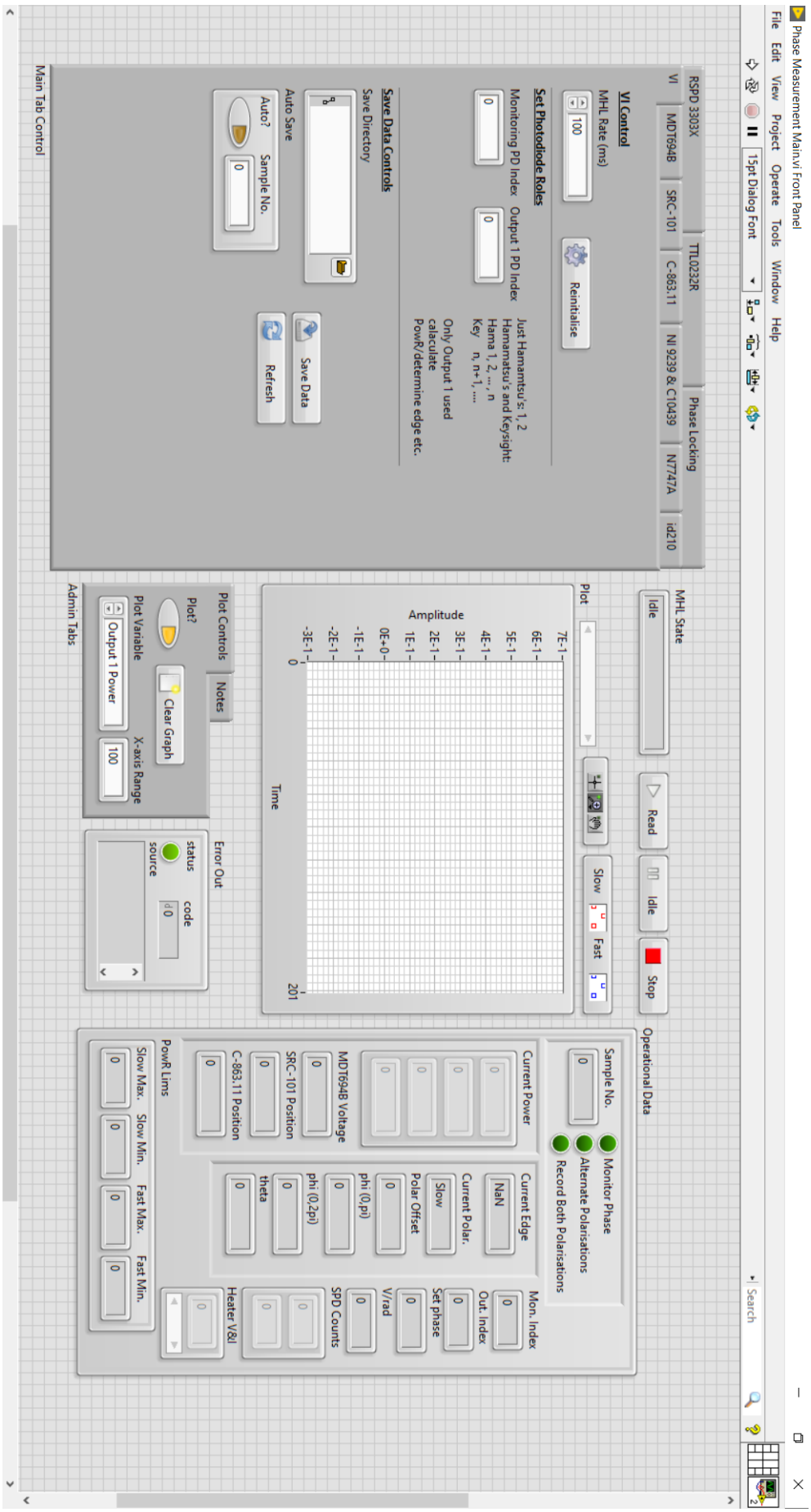


Figure C.2: Screenshot of the LabVIEW front panel of the main program, used to control the measurement system.

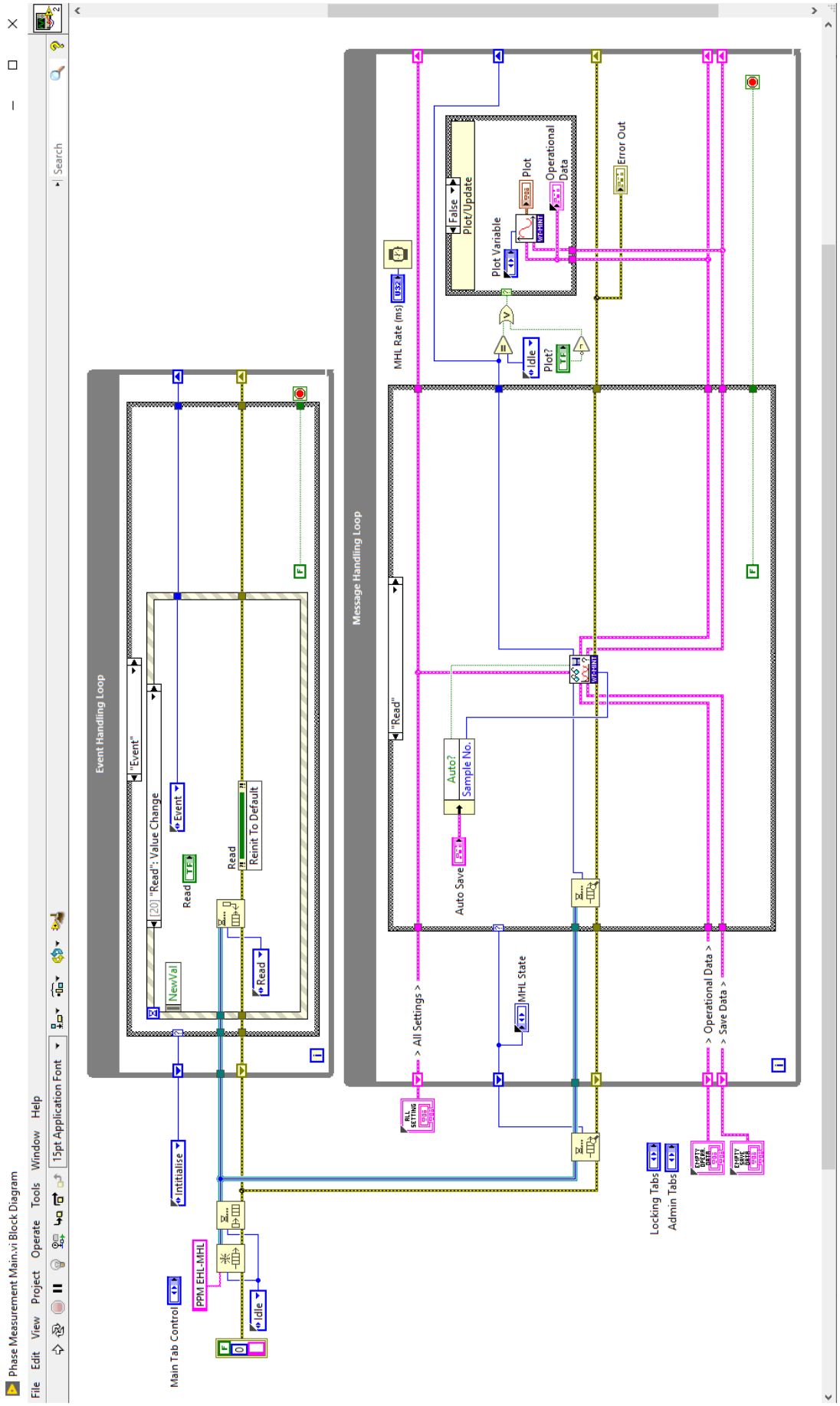


Figure C.3: Screenshot of the LabVIEW block diagram of the main program, used to control the measurement system.

C.2 Interpolating Peaks and Troughs

The method of identifying the maximum and minimum of the power ratio, P_{Rmax1} and P_{Rmin1}, varies depending on the increment of the piezo sweep used to generate the interference pattern. For 0.1 V increment sweeps, the resolution of the interference pattern produces a well resolved peak and trough, such that the value of P_{Rmax1} and P_{Rmin1} can be found from the data points directly. The is preferable to attempting to fit a function to the peak or trough due to the non-linear response of the peizo element with respect to phase, as well as general drift in the measurement system AMZI. These two properties result in non-symmetric peaks and troughs of the interference pattern, which is demonstrated by the repeated interference fringes shown in figure C.4. This data, used in section 4.1.1, is generated by sending the slow polarisation of the CW reference signal into the AMZI and performing multiple 0.1 V increment sweeps of the piezo voltage. The minimum and maximum data points corresponding to the peaks and troughs are identified and plotted in figure C.4 (crosses). The non-symmetric nature of some of the peaks and troughs can be seen clearly.

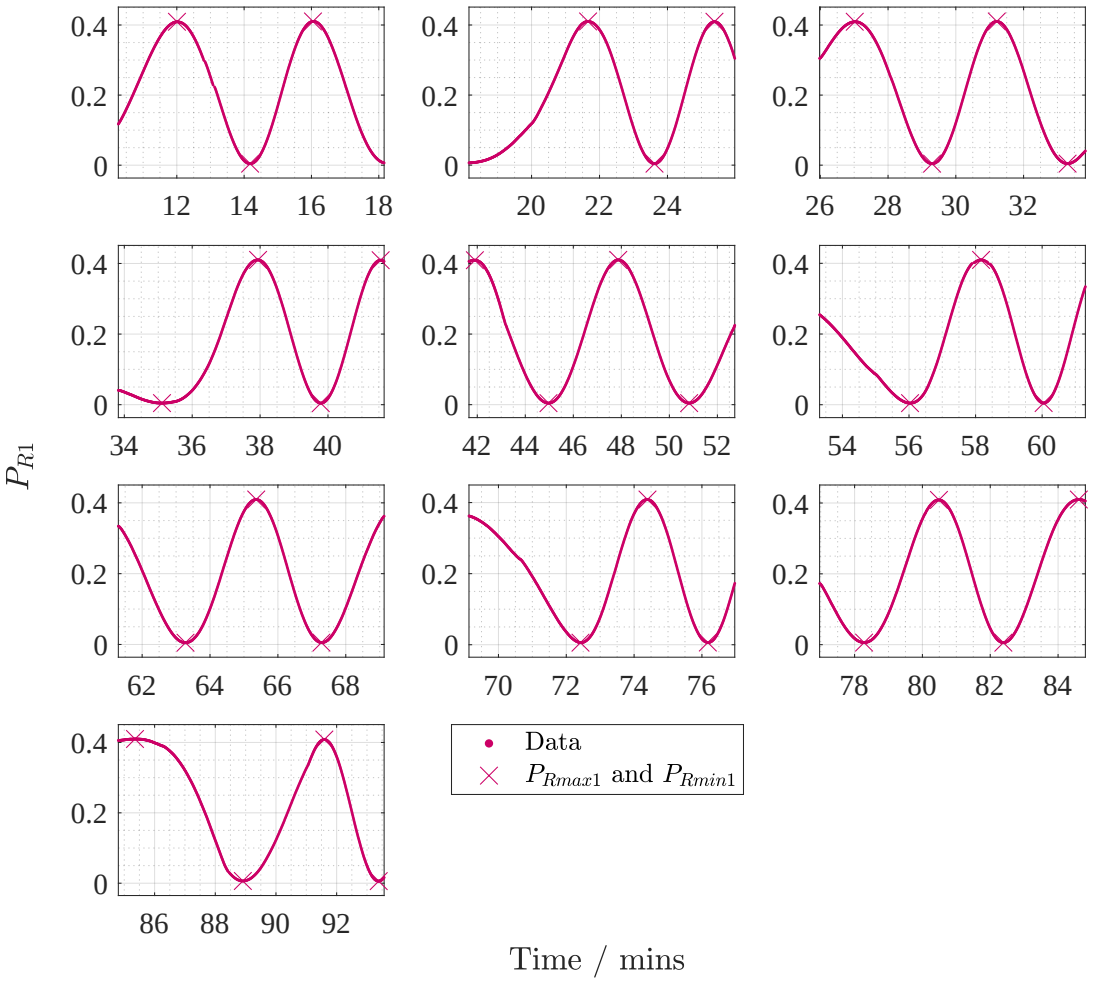


Figure C.4: Interference patterns of the slow reference signal for multiple up and down sweeps of the piezo voltage, with a 0.1 V incremental step. The data is the same as that used in section 4.1.1.

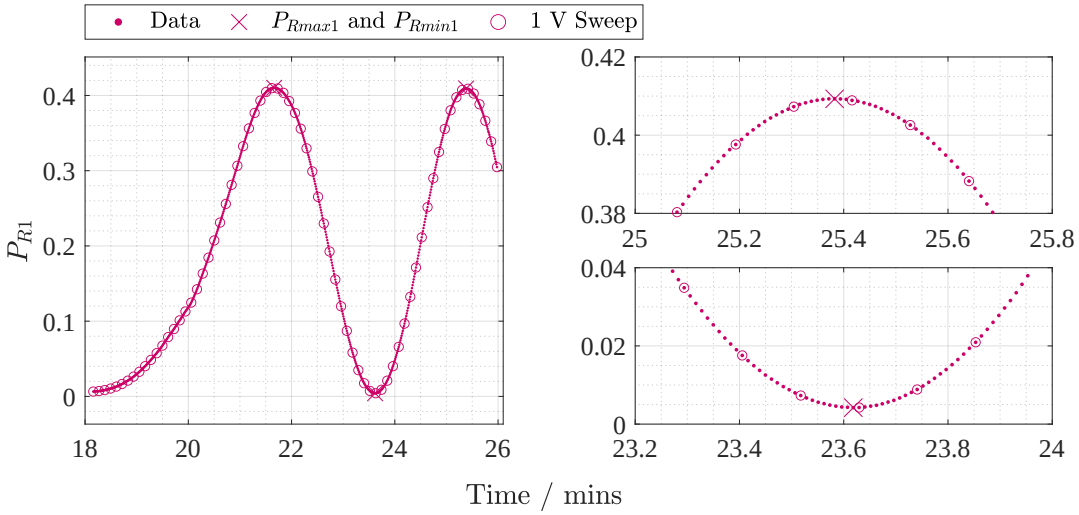


Figure C.5: Interference pattern of the centre top plot of figure C.4, resulting from a 0.1 V increment piezo sweep. Every tenth data point is circled, indicating the data points of a pseudo 1 V increment data sweep. The two plots on the right are magnifications of one peak and one trough from the pattern.

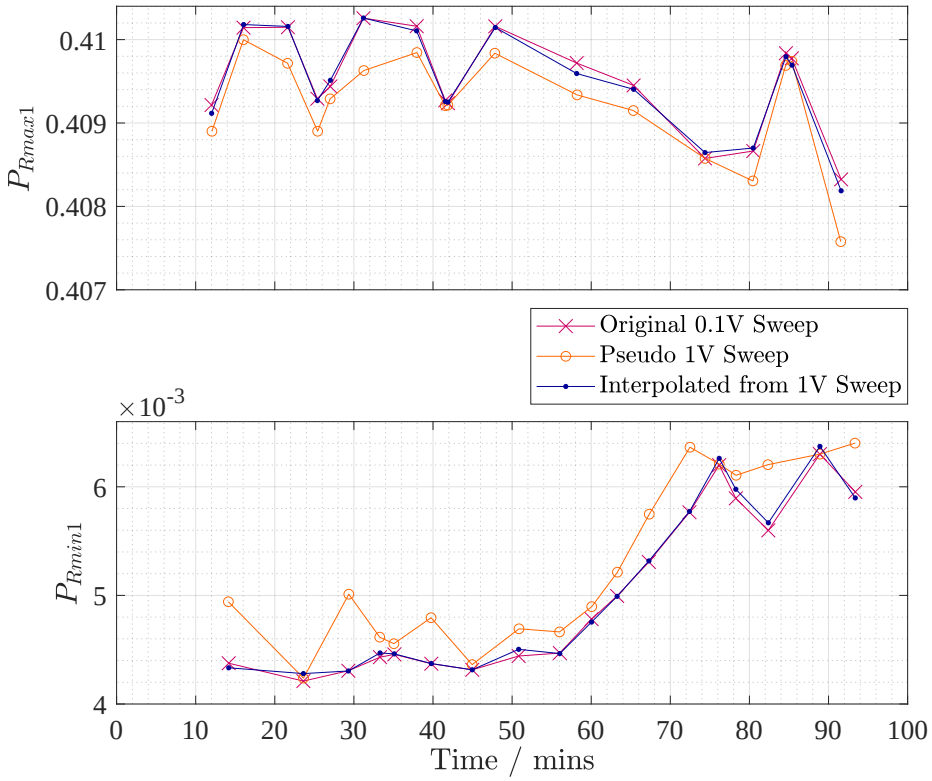


Figure C.6: Plots of P_{Rmax1} and P_{Rmin1} for the data shown in figure C.4. The values of P_{Rmax1} and P_{Rmin1} are calculated directly from the maximum and minimum of the 0.1 V incremental sweep data, directly from the maximum and minimum of the pseudo 1 V increment sweep data and from the maximum and minimum of the parabolas fit to the pseudo 1 V sweep data.

However, for 1 V increment piezo sweeps, the resolution is not sufficient to provide appropriate estimates for the values of P_{Rmax1} and P_{Rmin1}. For these sweeps, a parabola is fit to the closest four data points to a peak or trough, and the maximum or minimum of that fit is used to estimate P_{Rmax1} or P_{Rmin1} respectively. To demonstrate the effectiveness of this approach, the interference pattern shown in the centre top plot of figure C.4 is replotted in figure C.5. To simulate a 1 V increment piezo sweep from this 0.1 V increment sweep, every tenth data point is circled, also shown in figure C.5. The magnified plots to the right demonstrate the resolution provided by a 0.1 V increment sweep compared to a 1 V increment sweep. The maximum and minimum data points of the 0.1 V increment sweep corresponding to peaks and troughs are identified. The maximum and minimum data points of the pseudo 1 V increment sweep corresponding to the peaks and troughs are also identified, and a parabola is fit to the closest four points surrounding each peak and trough. This is completed for all sweeps shown in figure C.4 and the values of P_{Rmax1} and P_{Rmin1} found are plotted in figure C.6. This shows that the interpolated values of P_{Rmax1} and P_{Rmin1}, calculated by fitting a parabola to the pseudo 1 V increment sweep data, are very similar to the values found directly from the data points of the 0.1 V increment sweep data. Whereas, in comparison, the values of P_{Rmax1} and P_{Rmin1} taken directly from the data points of the pseudo 1 V increment sweep are varied compared to that for the 0.1 V increment sweep. Therefore, applying this interpolation method to the 1 V data sweeps is justified.

C.3 Calculated Phase Uncertainty

C.3.1 Uncertainty in $\Delta\psi_{IntR\,[0,\pi]}$

The equation for the interferometer phase bounded between $[0, \pi]$, for either the slow or fast polarised reference signal is given by,

$$\psi_{IntR\,[0,\pi]} = \cos^{-1}\left(\frac{1}{D_{1R}}\left[S_{1R} - 2\frac{P_{1R}}{P_{MR}}\right]\right). \qquad \text{(2.38, revisited)}$$

The uncertainty in the power ratio, $\frac{P_{1R}}{P_{MR}}$, is estimated on inspection of the data. The uncertainty in the sum and difference terms is calculated as follows. For multiple interference patterns, the uncertainty in the maximum and minimum of the power ratio is given by,

$$\sigma_{P_{Rmax1}} = \sqrt{\frac{1}{n-1}\sum_n \left(P_{Rmax1} - \mu_{P_{Rmax1}}\right)^2}$$
$$\sigma_{P_{Rmin1}} = \sqrt{\frac{1}{n-1}\sum_n \left(P_{Rmin1} - \mu_{P_{Rmin1}}\right)^2}$$

where n is the number of data points and $\mu_{P_{Rmax1}}$ and $\mu_{P_{Rmin1}}$ are the mean values of P_{Rmax1} and P_{Rmin1} respectively. The sum and difference terms are given by,

$$S_{1R} = P_{Rmax1} + P_{Rmin1}$$
$$D_{1R} = P_{Rmax1} - P_{Rmin1}$$

and the resulting uncertainty equations for these terms are,

$$\sigma_S = \sigma_D = \sigma_{P_{Rmax}} + \sigma_{P_{Rmin}} + \sigma_{P_{R(piezo)}}$$

where $\sigma_{P_{R(piezo)}}$ is the uncertainty in the power ratio resulting from the transmittance change during a piezo sweep.

To calculate the total uncertainty for $\psi_{IntR\,[0,\pi]}$, it is first useful to perform the following substitution for the inverse cosine argument,

$$u = \frac{1}{D_{1R}}\left(S_{1R} - 2\frac{P_{1R}}{P_{MR}}\right) \qquad \text{(3.10, revisited)}$$

such that,

$$\psi_{IntR\,[0,\pi]} = \cos^{-1}(u).$$

The uncertainty of the inverse cosine argument, u, can be calculated and is given by,

$$\begin{aligned}\sigma_u &= \frac{1}{D_{1R}}\left(S_{1R} - 2\frac{P_{1R}}{P_{MR}}\right)\left(\frac{\sigma_{D_{1R}}}{D_{1R}} + \frac{2\sigma_{P_{1R}/P_{MR}} + \sigma_{S_{1R}}}{S_{1R} - 2\frac{P_{1R}}{P_{MR}}}\right) \\ &= \frac{1}{D_{1R}^2}\left[\left(S_{1R} - 2\frac{P_{1R}}{P_{MR}}\right)\sigma_{D_{1R}} + D_{1R}\left(2\sigma_{P_{1R}/P_{MR}} + \sigma_{S_{1R}}\right)\right] \qquad \text{(3.11, revisited)}\end{aligned}$$

and the uncertainty of the interferometer phase is therefore given by,

$$\sigma_{\Delta\psi_{IntR\,[0,\pi]}} = \frac{-1}{\sqrt{1-u^2}}\sigma_u. \qquad \text{(3.9, revisited)}$$

Appendix D

Appendices for Chapter 4

D.1 Phase Analysis Code

D.1.1 Code Overview

The analysis of experimental data is performed using a home made MATLAB code, a snapshot of which is shown in figure D.1. The code performs the following tasks:

- Defines voltage sweeps
- Identifies and interpolates peaks and troughs of interference patterns (see section 3.3.2)
- Calculates $\Delta\psi_{[0,\pi]}$, $\Delta\psi_{[0,2\pi)}$ and $\Delta\theta$ for the reference signal and the signal under test (see section 3.3.2)
- References $\Delta\theta_{IntRS}$ and $\Delta\theta_{IntRF}$ between piezo sweeps
- Calculates the phase offset (see section 3.3.2)
- Determines $\Delta\theta_{IntR}$ (see section 3.4.2)
- Determines $\Delta\theta_{IntQ}$ (see section 2.4.3)
- Calculates the phase of the signal under test

Many of these operations are completed automatically by the code, and various elements can be enabled or disabled depending on the dataset, for example peak interpolation can be skipped for data sets involving 0.1 V incremental piezo sweeps. Elements of the analysis have already been detailed in the text of the main chapters, and the corresponding sections are noted in the list above. The only remaining significant step of the analysis not currently detailed is the phase referencing between piezo sweeps, which is explored in the following section.

D.1.2 Phase Referencing between Piezo Sweeps

For each sweep of the piezo voltage performed, the change in the interferometer phase can be calculated and unwrapped using the two polarisations of the reference signal. This ultimately results in the data sets of $\Delta\theta_{IntRS}$ for the slow polarisation and $\Delta\theta_{IntRF}$ for the fast polarisation, which define the total change in the phase difference between the AMZI arms over the course of the piezo sweep. However, this calculated phase change is independent from those calculated for other sweeps of the piezo. Therefore, to accurately map the change in the interferometer phase across an entire experiment consisting of many

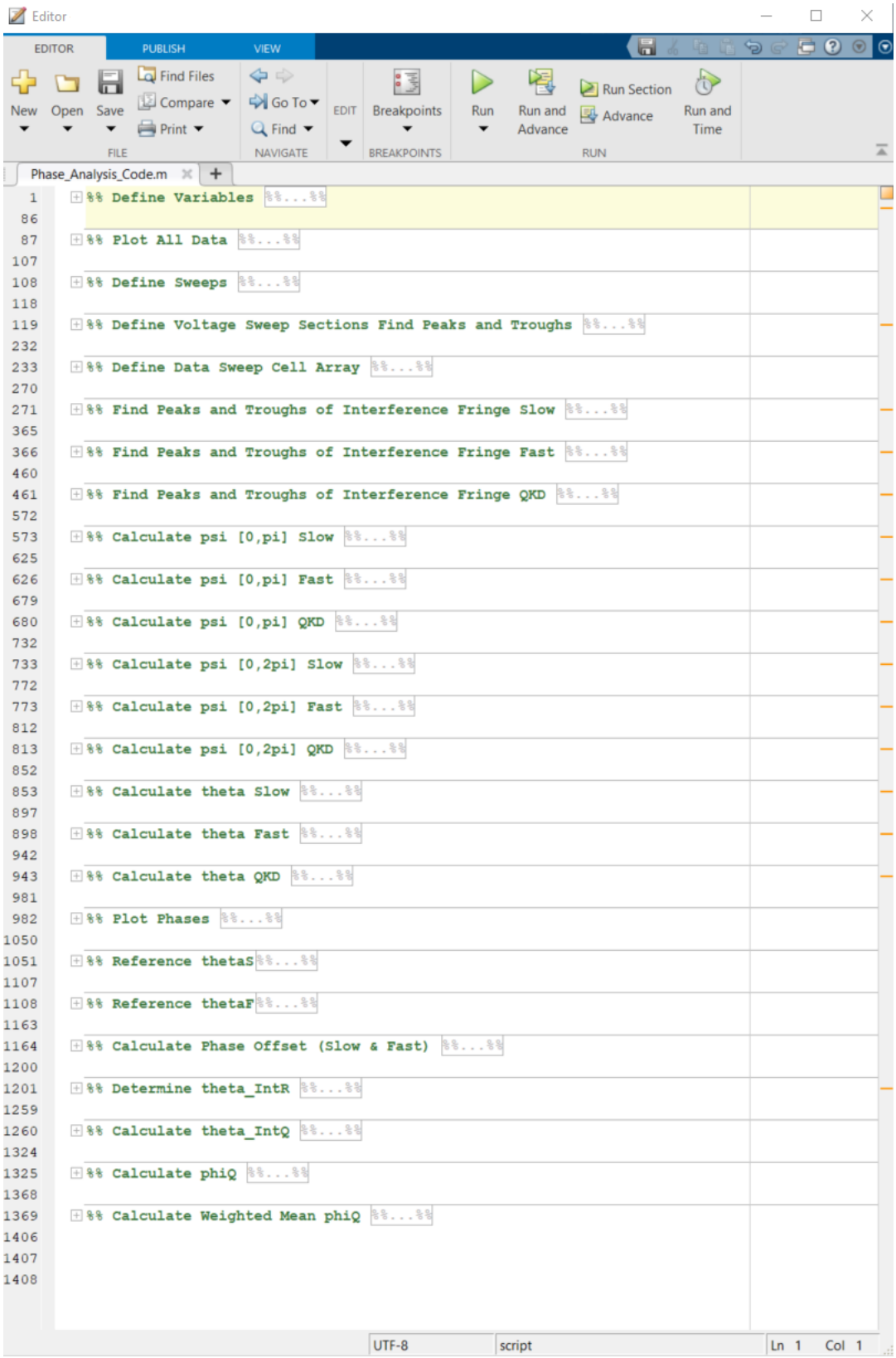


Figure D.1: Snapshot of the MATLAB phase analysis code.

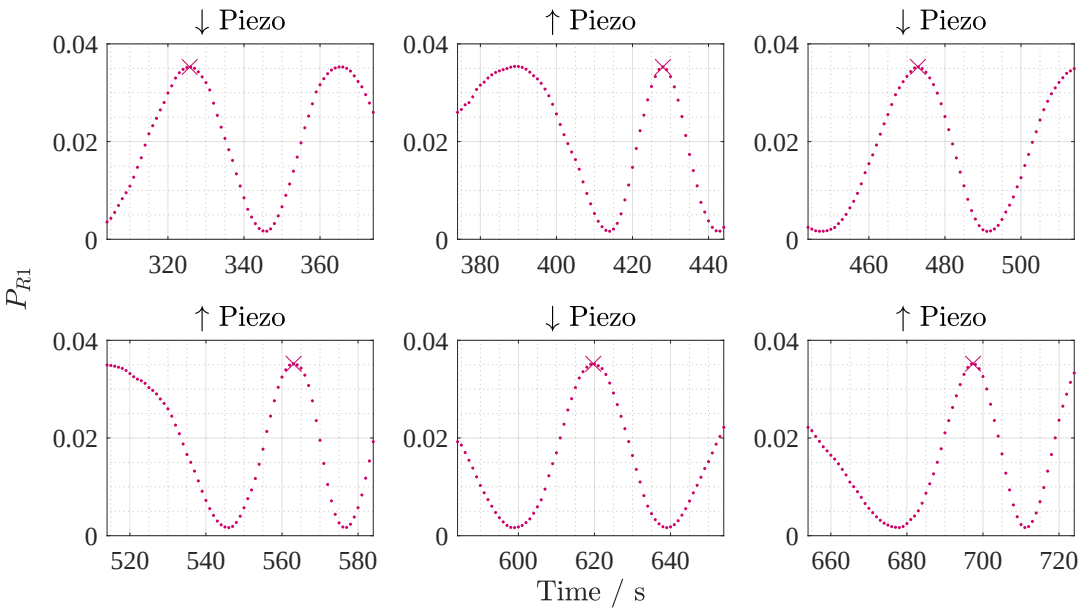


Figure D.2: The interference patterns of the power ratio (P_{R1}) for six sweeps of the piezo voltage, where each plot corresponds to one of the sweeps. The voltage sweeps alternate in direction, where ↑ Piezo indicates a voltage sweep from 0 V to 70 V and ↓ Piezo indicates a voltage sweep from 70 V to 0 V. The sweeps occur in order from left to right, top to bottom, as indicated by the time on the x-axis. The crosses indicate the interpolated peaks of the interference pattern that are used to reference the phases between each sweep.

piezo sweeps, the change in the interferometer phase must be referenced according to the other sweeps.

The piezo voltage sweeps are performed one after another in alternating directions, where an upwards sweep (↑ Piezo) is typically from 0 V to 70 V, and a downwards sweep (↓ Piezo) is typically from 70 V to 0 V. Figure D.2 shows the interference patterns of the slow polarisation of the reference signal resulting from six sweeps of the piezo voltage. Each sweep is a separate plot of the figure, where the title of each plot indicates the direction of the piezo sweep. The data used here is from the experiment assessing the coherence of a pulsed laser in section 4.2. As the sweeps occur soon after one another, the same peaks and troughs in each pattern can be seen in each trace, where for example, due to the alternating directions of the sweeps, the first peak in the top left plot corresponds to the second peak in the top centre plot, as marked by the crosses. The cross on each plot indicates a common peak between each of the sweeps, where at this point the OPD between the two of the arms of the AMZI is the same for each sweep. This common point can therefore be used to reference the phases calculated for each sweep of the piezo voltage.

The calculated unwrapped phases for the slow ($\Delta\theta_{IntRS}$) and fast ($\Delta\theta_{IntRF}$) polarisations of the reference signal are shown in the top plot of figure D.3. The plot also shows crosses at the phase values corresponding to the peaks, where these phase values are multiples of 2π. For the slow signal, these points are the same as those shown in figure D.2. The phases corresponding to each of the six piezo sweeps can be seen clearly, where these are each disjointed and independent from one another. As the cross marked peaks are physically the same OPD of the AMZI, these points are used to reference the sweeps according to one another. The resulting referenced phases for each sweep are shown in the bottom plot of figure D.3.

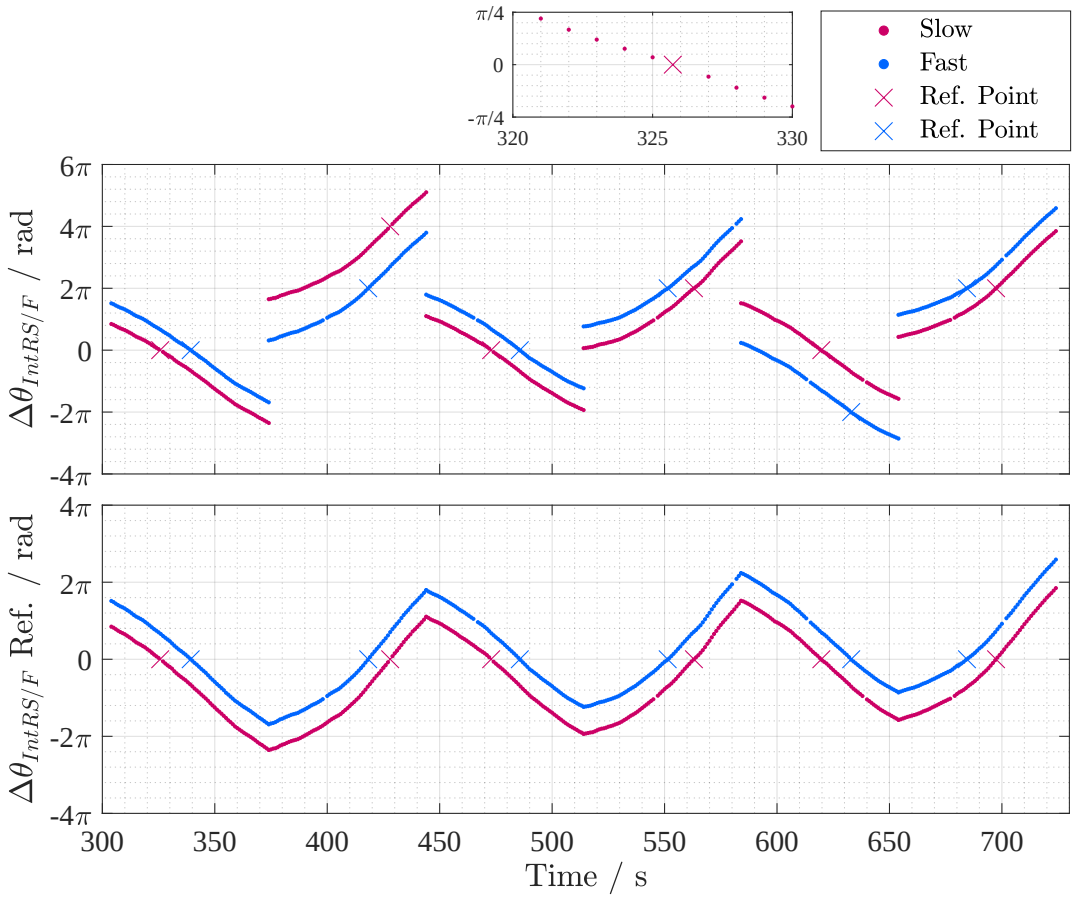


Figure D.3: Plots of the change in the interferometer phase $\Delta\theta_{IntRS}$ and $\Delta\theta_{IntRF}$ calculated by the slow and fast polarisations of the reference signal respectively for six alternating sweeps of the piezo voltage. The top plot shows the phases prior to referencing, where the phases of each sweep are independent. Crosses mark the phases of the interference pattern peaks used to reference the sweeps with one another, where these phases correspond to multiples of 2π. The magnification plot shown above corresponds to the cross mark on the first piezo sweep, highlighting how the interpolated peak lies along the phase plot. The bottom plot shows the phases after they have been referenced (Ref.) according to these peaks, such that the resulting reference points all lie along zero.

The referenced interferometer phases are then used to calculated the offset in between the two signals, which then in turn allows the final interferometer phase $\Delta\theta_{IntR}$ dataset to be compiled.

D.2 Estimate the Maximum and Minimum Power Ratio

The power ratios pertaining to sending light through just the internal arm of the AMZI, $P_{R1\,Int}$, and just the external arm of the AMZI, $P_{R1\,Ext}$, can be used to estimate the maximum and minimum of the interference pattern, P_{Rmax1} and P_{Rmin1}. Using the following equations from appendix B.2.4,

$$S_1 = P_{Rmax1} + P_{Rmin1} = 2\frac{\eta_1}{\eta_M}\frac{T_0}{R_0}\left(\eta_a T_1 T_2 + \eta_b R_1 R_2\right) \quad \text{(B.3, revisited)}$$

$$D_1 = P_{Rmax1} - P_{Rmin1} = 4\frac{\eta_1}{\eta_M}\frac{T_0}{R_0}\sqrt{\eta_a\eta_b T_1 T_2 R_1 R_2}\int_{-\infty}^{\infty} G_{(k+1)a}G_{kb}dt \quad \text{(B.4, revisited)}$$

$$P_{R1} = \frac{1}{2}\left[S_1 - D_1\cos\left(\phi_Q + \psi_{Int}\right)\right] \quad \text{(2.14, revisited)}$$

and taking the internal arm of the measurement system AMZI as interferometer arm a, and the external arm as arm b, the equations above simplify as follows. Firstly, when the signals are propagated through only the internal arm, where the external arm is blocked ($\eta_b = 0$), the equations are written as,

$$\begin{aligned} S_{1\,Int} &= 2\frac{\eta_1}{\eta_M}\frac{T_0}{R_0}\eta_a T_1 T_2 \\ D_{1\,Int} &= 0 \\ P_{R1\,Int} &= \frac{\eta_1}{\eta_M}\frac{T_0}{R_0}\eta_a T_1 T_2. \end{aligned}$$

Alternatively, when the signals are propagated through only the external arm, where the internal arm is blocked ($\eta_a = 0$), the equations can be written as,

$$\begin{aligned} S_{1\,Ext} &= 2\frac{\eta_1}{\eta_M}\frac{T_0}{R_0}\eta_b R_1 R_2 \\ D_{1\,Ext} &= 0 \\ P_{R1\,Ext} &= \frac{\eta_1}{\eta_M}\frac{T_0}{R_0}\eta_b R_1 R_2. \end{aligned}$$

When the signals can propagate through both arms of the AMZI, the internal only and external only equations can be substituted in as follows,

$$\begin{aligned} S_1 &= 2\frac{\eta_1}{\eta_M}\frac{T_0}{R_0}\left(\eta_a T_1 T_2 + \eta_b R_1 R_2\right) \\ &= 2\left(P_{R1\,Int} + P_{R1\,Ext}\right) \end{aligned}$$

$$\begin{aligned} D_1 &= 4\frac{\eta_1}{\eta_M}\frac{T_0}{R_0}\sqrt{\eta_a\eta_b T_1 T_2 R_1 R_2}\int_{-\infty}^{\infty} G_{(k+1)a}G_{kb}dt \\ &= 4\sqrt{P_{R1\,Int}P_{R1\,Ext}}\int_{-\infty}^{\infty} G_{(k+1)a}G_{kb}dt \\ &\approx 4\sqrt{P_{R1\,Int}P_{R1\,Ext}} \end{aligned}$$

where the final approximation for the expression of D_1 assumes that there is good pulse overlap, such that the integral of the Gaussian functions is ≈ 1. As S_1 and D_1 are the sum and difference of the maximum and minimum power ratio of the interference pattern,

the following equations can be obtained,

$$\begin{aligned} P_{Rmax1} &= \frac{1}{2}(S_1 + D_1) \\ &\approx P_{R1\,Int} + P_{R1\,Ext} + 2\sqrt{P_{R1\,Int}P_{R1\,Ext}} \\ P_{Rmin1} &= \frac{1}{2}(S_1 - D_1) \\ &\approx P_{R1\,Int} + P_{R1\,Ext} - 2\sqrt{P_{R1\,Int}P_{R1\,Ext}}. \end{aligned}$$

Therefore the maximum and minimum power ratio of an interference pattern can be approximated using the power ratio from the internal arm only and external arm only power ratio values.

References

[1] H Delfs and H Knebl, *Introduction to Cryptography Principles and Applications*, 3rd ed., Springer, 2015.

[2] Simon Singh, *The code book: the secret history of codes and codebreaking*, Fourth Estate, 1999.

[3] R L Rivest, A Shamir, and L Adleman, *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, Commun. ACM, 21, (2), 1978, 120–126.

[4] N Koblitz, *Elliptic Curve Cryptosystems*, Mathematics of Computation, 48, (177), 1987, 203–209.

[5] V S Miller, *Use of Elliptic Curves in Cryptography*, Advances in Cryptology CRYPTO '85 Proceedings, 1986, 417–426.

[6] P W Shor, *Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer*, SIAM Journal on Computing, 26, (5), 1997, 1484–1509.

[7] P W Shor, *Algorithms for quantum computation: discrete logarithms and factoring*, Proceedings 35th Annual Symposium on Foundations of Computer Science, 2002, 124–134.

[8] L Chen et al., *Report on Post-Quantum Cryptography*, NIST, 2016.

[9] G S Vernam, *Cipher Printing Telegraph Systems For Secret Wire and Radio Telegraphic Communications*, Transactions of the American Institute of Electrical Engineers, XLV, 1926, 295–301.

[10] M J Dworkin et al., *Advanced Encryption Standard (AES)*, Federal Inf. Process. Stds. (NIST FIPS), 197, 2001.

[11] L K Grover, *A fast quantum mechanical algorithm for database search*, Proceedings, 28th Annual ACM Symposium on the Theory of Computing (STOC), 1996, 212–219.

[12] M Mosca, *The context of quantum security*, IDQ Winter School, 2019.

[13] V Mavroeidis et al., *The impact of quantum computing on present cryptography*, International Journal of Advanced Computer Science and Applications, 9, (3), 2018, 405–414.

[14] M Mosca, *What's your risk from quantum computers?*, https://open-ecosystem.org/articles/whats-your-risk-quantum-computers, 2021.

[15] D J Bernstein and T Lange, *Post-quantum cryptography*, Nature, 549, (7671), 2017, 188–194.

[16] E Diamanti, *Continuous-variable QKD*, IDQ Winter School, 2019.

[17] C H Bennett and G Brassard, *Quantum cryptography: public key distribution and coin tossing*, Proc. 1984 IEEE International Conference on Computers, Systems, and Signal Processing, 1, 1984, 175–179.

[18] ETSI, *Quantum Safe Cryptography and Security*, White Paper, 8, 2015.

[19] K Inoue, *Quantum key distribution technologies*, IEEE Journal of Selected Topics in Quantum Electronics, 12, (4), 2006, 888–896.

[20] Marco Lucamarini et al., *Implementation Security of Quantum Cryptography*, 27, 2018.

[21] M. D. Eisaman et al., *Invited Review Article: Single-photon sources and detectors*, Review of Scientific Instruments, 82, (7), 2011, 71101.

[22] C J Chunnilall et al., *Metrology of single-photon sources and detectors: a review*, Optical Engineering, 53, (8), 2014, 1–17.

[23] N Gisin et al., *Quantum Cryptography*, Reviews of Modern Physics, 74, (1), 2002, 145–195.

[24] R J Glauber, *Coherent and Incoherent States of the Radiation Field*, Phys. Rev. 131, (6), 1963, 2766–2788.

[25] T Kobayashi, A Tomita, and A Okamoto, *Evaluation of the phase randomness of a light source in quantum-key-distribution systems with an attenuated laser*, Phys. Rev. A, 90, 3 2014, 032320.

[26] W Hwang, *Quantum Key Distribution with High Loss: Toward Global Secure Communication*, Physical Review Letters, 91, (5), 2003, 57901.

[27] H Lo, X Ma, and K Chen, *Decoy State Quantum Key Distribution*, Physical Review Letters, 94, (23), 2005, 1–5.

[28] X Wang, *Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography*, Physical Review Letters, 94, (23), 2005, 230503.

[29] D Stucki et al., *Fast and simple one-way quantum key distribution*, Applied Physics Letters, 87, (19), 2005, 1–3.

[30] K Inoue, E Waks, and Y Yamamoto, *Differential-phase-shift quantum key distribution using coherent light*, Physical Review A, 68, (2), 2003, 022317.

[31] K Inoue and Y Iwai, *Differential-quadrature-phase-shift quantum key distribution*, Phys. Rev. A, 79, (2), 2009, 22319.

[32] T Sasaki, Y Yamamoto, and M Koashi, *Practical quantum key distribution protocol without monitoring signal disturbance*, Nature, 509, (7501), 2014, 475–478.

[33] H Lo, M Curty, and B Qi, *Measurement-Device-Independent Quantum Key Distribution*, Physical Review Letters, 108, (13), 2012, 130503.

[34] M Lucamarini et al., *Overcoming the rate–distance limit of quantum key distribution without quantum repeaters*, Nature, 557, (7705), 2018, 400–403.

[35] D Gottesman et al., *Security of quantum key distribution with imperfect devices*, Quantum Information and Computation, 4, (5), 2004, 325–360.

[36] Z Cao et al., *Discrete-phase-randomized coherent state source and its application in quantum key distribution*, New Journal of Physics, 17, (5), 2015, 53014.

[37] Z L Yuan et al., *Robust random number generation using steady-state emission of gain-switched laser diodes*, Applied Physics Letters, 104, 2014, 261112.

[38] Z L Yuan et al., *Directly Phase-Modulated Light Source*, Phys. Rev. X, 6, (3), 2016, 31044.

[39] J C Boileau et al., *Robust Polarization-Based Quantum Key Distribution over a Collective-Noise Channel*, Phys. Rev. Lett. 92, (1), 2004, 17901.

[40] N Jain et al., *Trojan-horse attacks threaten the security of practical quantum cryptography*, New Journal of Physics, 16, (12), 2014, 123030.

[41] ETSI, *Quantum Key Distribution (QKD); Component characterization: characterizing optical components for QKD systems*, 1, 2016, 136.

[42] M Loeffler et al., *Current Standardisation Landscape and existing Gaps in the Area of Quantum Key Distribution*, https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/horizon-results-platform/29227, 2021.

[43] ISO/IEC, *ISO/IEC CD 23837-2.2 Information technology security techniques - Security requirements, test and evaluation methods for quantum key distribution - Part 2: Evaluation and testing methods*, https://www.iso.org/standard/77309.html, 2021.

[44] ETSI, *ISG QKD Activity Report 2020*, https://www.etsi.org/committee-activity/activity-report-qkd, 2020.

[45] C J Chunnilall, Personal Communication, 2017 - 2021.

[46] U Leonhardt and H Paul, *Measuring the quantum state of light*, Progress in Quantum Electronics, 19, (2), 1995, 89–130.

[47] T P Spiller, Personal Communication and Notes on Quantum Field Theory (unpublished), 2017 - 2021.

[48] A Steimacher et al., *The temperature coefficient of the optical path length as a function of the temperature in different optical glasses*, Journal of Non-Crystalline Solids, 348, 2004, 240–244.

[49] B Edlén, *The Refractive Index of Air*, Metrologia, 2, (2), 1966, 71–80.

[50] K P Birch and M J Downs, *An Updated Edlén Equation for the Refractive Index of Air*, Metrologia, 30, (3), 1993, 155–162.

[51] K P Birch and M J Downs, *Correction to the Updated Edlén Equation for the Refractive Index of Air*, Metrologia, 31, (4), Jan. 1994, 315–316.

[52] J A Stone and J H Zimmerman, *Index of Refraction of Air*, https://emtoolbox.nist.gov/Wavelength/Documentation.asp, 2004.

[53] A V Smith, J J Smith, and B T Do, *Thermo-optic and thermal expansion coefficients of RTP and KTP crystals over 300-350 K*, ArXiv e-prints, 2016, arXiv:1607.03964.

[54] D B Leviton and B J Frey, *Temperature-dependent absolute refractive index measurements of synthetic fused silica*, arXiv e-prints, 2008, arXiv:0805.0091.

[55] Corning Inc., *Corning HPFS 7979, 7980, 8655 Fused Silica Optical Materials Product Information*, https://www.corning.com/media/worldwide/csm/documents/HPFS_Product_Brochure_All_Grades_2015_07_21.pdf, 2015.

[56] Wavelength Electronics, *PTC5K-CH Temperature Controller*, https://www.teamwavelength.com/product/ptc5k-ch-5-a-temperature-controller-chassis-mount/, 2021.

[57] Thorlabs Tech Support, Personal Communication, 2019-2021.

[58] M J Hamp et al., *Investigation into the temperature dependence of chromatic dispersion in optical fiber*, IEEE Photonics Technology Letters, 14, (11), 2002, 1524–1526.

[59] P S Andre, A N Pinto, and J L Pinto, *Effect of temperature on the single mode fibers chromatic dispersion*, Proceedings of the 2003 SBMO/IEEE MTT-S International Microwave and Optoelectronics Conference - IMOC 2003, 1, 2003, 231–234.

[60] G Jotzu et al., *Continuous phase stabilization and active interferometer control using two modes*, Journal of Modern Optics, 59, (1), 2012, 42–45.

[61] A Tchebotareva et al., *Entanglement between a Diamond Spin Qubit and a Photonic Time-Bin Qubit at Telecom Wavelength*, Phys. Rev. Lett. 123, (6), 2019, 63601.

[62] Kylia, *About Us*, https://kylia.com/about-us, 2021.

[63] Kylia, *Delay Line Interferometers MINT and WT-MINT*, https://kylia.com/api-website-feature/files/download/11118/datasheet-MINT-V12.pdf, 2021.

[64] Bernhard Halle Nachfl. GmbH, *Soleil-Babinet Compensators*, https://www.b-halle.de/products/retarders/soleil_babinet_compensators.html, 2021.

[65] Physik Instrumente, *M-230 High-Resolution Linear Actuator with DC and Stepper Motor*, https://www.physikinstrumente.co.uk/en/products/linear-actuators/linear-actuators-with-stepper-dc-servo-motors/m-230-high-resolution-linear-actuator-with-dc-and-stepper-motor-703400/, 2021.

[66] Physik Instrumente, *C-863 Mercury Servo Controller*, https://www.physikinstrumente.co.uk/en/products/controllers-and-drivers/motion-controllers-drivers-for-linear-torque-stepper-dc-servo-motors/c-863-mercury-servo-controller-900606/, 2021.

[67] National Instruments, *Using a Queued Message Handler in LabVIEW*, https://www.ni.com/en-gb/support/documentation/supplemental/21/using-a-queued-message-handler-in-labview.html, 2021.

[68] National Instruments, *LabVIEW Front Panel Explained*, https://www.ni.com/en-gb/support/documentation/supplemental/08/labview-front-panel-explained.html, 2021.

[69] National Instruments, *LabVIEW Block Diagram Explained*, https://www.ni.com/en-gb/support/documentation/supplemental/08/labview-block-diagram-explained.html, 2021.

[70] PicoQuant, *Picosecond Pulsed Sources*, https://www.picoquant.com/products/category/picosecond-pulsed-sources/ldh-series-picosecond-pulsed-diode-laser-heads#specification, 2021.

[71] PicoQuant, *PDL 800-D Picosecond Diode Laser Driver*, https://www.picoquant.com/products/category/picosecond-pulsed-driver/pdl-800-d-picosecond-pulsed-diode-laser-driver-with-cw-capability, 2021.

[72] Thorlabs, *Ultrafast Fiber Optic Photodetectors*, https://www.thorlabs.com/newgrouppage9.cfm?objectgroup_id=10938&pn=DXM30AF#ad-image-0, 2021.

[73] Rio, *ORION 1550 nm Laser Module*, https://rio-lasers.com/1550-nm-laser-module/, 2021.

[74] IDQuantique, *ID210 Infrared Single-Photon Detector*, https://marketing.idquantique.com/acton/attachment/11868/f-50651fcb-ba83-43cd-b611-360e56191123/1/-/-/-/-/ID210/%20Product/%20Brochure.pdf, 2021.

[75] R Kirkwood, I P Degiovanni, and C Chunnilall, *Single-photon avalanche detectors: their characterisation and use in measuring single-photon pulses,* Proceedings in the 8th edition of the Single Photon Workshop, 2017.

[76] Thorlabs, *Pigtailed External Cavity (ECL) Single-Frequency Lasers, Butterfly Package*, https://www.thorlabs.com/newgrouppage9.cfm?objectgroup_id=4934&pn=SFL1550P#7260, 2021.

[77] EXFO, *T100S-HP - high-power continuously tunable laser*, https://www.exfo.com/en/products/lab-manufacturing-testing/optical-light-sources/t100s-hp/, 2021.

[78] Tektronix, *AWG70001A and AWG70002A*, https://www.tek.com/en/signal-generator/awg70000-arbitrary-waveform-generator-manual, 2021.

[79] Thorlabs, *12 W Laser Diode Temperature Controller*, https://www.thorlabs.com/newgrouppage9.cfm?objectgroup_id=307&pn=TED200C#8101, 2021.

[80] A Vaquero-Stainer et al., *Measurements towards providing security assurance for a chip-scale QKD system*, Proceedings, Quantum Technologies 2018, 10674, 2018, 145–152.

[81] D Subacius, A Zavriyev, and A Trifonov, *Fiber scattering limitations for quantum key distribution (QKD) system*, International Quantum Electronics Conference, 2004. (IQEC). 2004, 384–385.

[82] P Sibson et al., *Integrated silicon photonics for high-speed quantum key distribution*, Optica, 4, (2), 2017, 172–177.

[83] P. Sibson et al., *Chip-based quantum key distribution*, Nature Communications, 8, (13984), 2017, 1–6.

[84] J S Townsend, *A Modern Approach to Quantum Mechanics*, 2nd ed., University Science Books, 2012.