Continuous Variable Quantum Key Distribution in presence of emulated atmospheric turbulence and with passive eavesdropping

Emma Tien Hwai MEDLOCK

MSc BY RESEARCH

UNIVERSITY OF YORK

PHYSICS

August, 2021

UNIVERSITY OF YORK

Abstract

Physics

Master of Science by Research in Physics

Continuous Variable Quantum Key Distribution in presence of emulated atmospheric turbulence and with passive eavesdropping

by Emma Tien Hwai MEDLOCK

Atmospheric turbulence has the potential to disrupt quantum communication. Therefore, it is important to research the impact of such turbulence on free-space quantum key distribution. In this experiment the correlations between the two users, Alice and Bob ($\rho_{A,B}$), and between Alice and an eavesdropper, Eve, ($\rho_{A,E}$) were compared for a satellite to ground continuous variable quantum key distribution system, emulated in the lab. Here the atmospheric turbulence was emulated using a deformable mirror. Bob is considered to be at the centre of the beam at a ground station with passive Eve being displaced from the centre of the beam at a another ground station. It was found that Alice and Bob had better correlation than Alice and Eve, with both $\rho_{A,B}$ and $\rho_{A,E}$ decreasing with increasing atmospheric turbulence and $\rho_{A,E}$ decreasing the more Eve was displaced from the centre of the beam. The less correlated Alice and Eve are, the less information Eve has about the raw key. When Eve's information about the raw key is below a certain threshold, Alice can increase the signal power. Therefore the channel distance and key rate can be increased.

Contents

List of Tables

List of Figures

Acknowledgements

Special thanks to my parents, my supervisors Dr. Kumar and Prof. Spiller, as well as Dr. Konieczniak and Dr Mortzou. Thank you for all your help and support on this project. I am also grateful for the support of the Quantum Communications Hub.

Declaration of Authorship

I, Emma Tien Hwai MEDLOCK, 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

Quantum key distribution (QKD) refers to the process of establishing a secret key between two parties, Alice and Bob, via a quantum channel and supporting conventional communication, where Alice is the sender and Bob the receiver. In order to make this channel quantum, the key is either encoded into the discrete variables (DV) of the light or the continuous variables (CV) (Pirandola et al., 2020). For both DV and CV-QKD the information is encoded into the phase and amplitude of the light (Vagniluca et al., 2020). In DV-QKD the information is encoded into the quantum state of single photons, i.e. the discrete variables of the light. These can then be measured using photon detectors. For CV-QKD the information is encoded into the quadratures, i.e. the continuous variables of the light. These quantities will be defined in more detail in section 2.1.2.

Using the quantum nature of light to establish secret keys is desirable, since in conventional symmetric cryptography algorithms the communication security relies solely on the secrecy of the encryption key (Diamanti et al., 2016). Therefore, current cyber-security, which is based on classical methods, guarantees only some level of security. Additionally, with current cyber-security, it is impossible to detect an eavesdropper (Eve), i.e. detect additional noise in the channel that can be attributed to Eve. Classical public key cryptography solves this by relying on computational assumptions such as hardness of factoring. This does not provide informational security and is vulnerable to future advances in computational power. Using Shor's algorithm, used to find prime factors of large numbers efficiently (Shor, 1994), and quantum computers, this type of cryptography can be broken. In QKD on the other hand, keys can be distributed with information-theoretical security (Diamanti and Leverrier, 2015) and can be done regardless of the quantum power of Eve (Liang, Poor, Shamai, et al., 2009; Renner, Gisin, and Kraus, 2005). This is possible since Eve cannot keep a transcript of the quantum signals due to the quantum non-cloning theorem (Wootters and Zurek, 1982; Dieks, 1982) and QKD is therefore future proof. Another advantage of QKD over its classical counterpart is that it is impossible to eavesdrop without detection, as Eve can be detected as a disturbance of the transmission and so the key distributed is random and unknown to anyone else (Bennett and Brassard, 2020). Eve can intercept, measure and resend every pulse sent by Alice to Bob, but has to guess a random basis. This results in a 25% error rate in the key established between Alice and Bob, so eavesdropping can be monitored by keeping track of the error rate. If the error rate is above a certain threshold the channel can be interpreted as insecure. For QKD, the maximum key rates achievable depend on Alice and Bob's mutual information $I_{A,B}$, reconciliation efficiency ρ_r (reconciliation in CV-QKD can be seen in section 2.4.1) and the maximum information Eve can have $I_{Eve,max}$ (Grosshans and Grangier, 2002a). Alice and Bob's mutual information depends on the receiver and the signal power. Eve's maximum information depends

on the signal power, channel attenuation and excess noise. Alice and Bob's mutual information also depends on these parameters. The maximum key rates achievable in QKD are

$$I_{key,max} = \rho_r I_{A,B} - I_{Eve,max}. \tag{1.1}$$

QKD systems operate under real world conditions and fibre based QKD systems are already commercially available. The major hindrance of QKD for wide-spread use is currently the transmission distances as well as cost. Therefore achieving secure key rates over larger distances are limited, as transmittance losses increase exponentially with increasing distance (Bedington, Arrazola, and Ling, 2017). This led to the introduction of satellite QKD. Atmosphere has an attenuation of $0.07dB/km$ at $2400m$ above sea-level compared to fibre with an attenuation of $0.18dB/km$. Above Earth's atmosphere, in the vacuum of space, the attenuation become negligible. This means satellite QKD can increase the distances at which secure key rates are achieved at. Currently the longest distance QKD system was established by a Chinese satellite in 2017 (Liao et al., 2017). They sent a secure key $1200km$ from a satellite to ground station with a key rate of $91bps$.

A large reason for the implementation of CV-QKD over DV-QKD is due to some of the technical challenges of DV-QKD. In DV-QKD the performance of the photodetectors are limited in terms of speed and efficiency in the single photon regime (Leverrier et al., 2008; Shen et al., 2014; Xu-Yang et al., 2013). In comparison CV-QKD allows the performance of QKD with very high key rates, at shorter distances while comparing to DV-QKD, as well as being able to be implemented using classical communication devices, with suitable quantum light signals (Jouguet et al., 2013; Wang et al., 2017; Jouguet, Kunz-Jacques, and Leverrier, 2011; Huang et al., 2016). Here the homodyne and heterodyne detection techniques are used in classical optical communication (these detection techniques will be defined in more detail in section 2.2). These systems will be compatible with standard wavelength division and multiplexed telecommunication networks. Additionally, the use of a strong Local Oscillator (LO) employed in coherent detection acts as a natural and extremely selective filter which can suppress noise photons at other wavelengths effectively (Qi et al., 2015). An LO is used in both homodyne and heterodyne detection to measure the quadratures against and is a classical signal. The filtering affect of the LO is due to interfromatic nature of homodyne and heterodyne detection (Pirandola, 2021). The detector creates a narrow filter by interfering the signal and LO close to the time-bandwidth product. Therefore CV-QKD can securely distribute a key over a noisy channel, although CV-QKD does require that the transmission of the optical line between Alice and Bob is larger than 50% (Hirano et al., 2017). If it is less, Eve can obtain a higher Signal to Noise Ratio (SNR) than Bob by replacing his lossy channel with her lossless channel. This is true only for direct reconciliation, the 50% loss limit can be overcome using reverse reconciliation. Another downside of CV-QKD arises due to the complex post-processing procedures related to error correction of the key Alice and Bob distil.

Passive eavesdropping refers to an eavesdropper, who passively overhears the signal sent but does not modify these or actively attack the channel (Ding et al., 2020; Ralph and Lam, 2013; Zhou and Shrestha, 2013). In fibre QKD Eve's receiver must be in between Alice and Bob to measure and intercept the states sent by Alice, this

can also be done in free space QKD. Bob and Alice can detect Eve's presence using the shot noise, if Eve is detected the channel will be interpreted as insecure and Alice and Bob will break off the protocol (Qin, Huang, and Makarov, 2017; Bennett and Brassard, 2020). This makes passive eavesdropping nonviable for such a scenario under real world conditions. Due to beam widening in free space QKD (Wang et al., 2018a), it is possible to place Eve's receiver on the same plane as Bob rather than in between Alice and Bob. Therefore, Eve's eavesdropping can go undetected making passive eavesdropping viable for free space QKD under real world conditions. Although, due to atmospheric turbulence, phase changes will occur in a free space channel changing the the results Eve will have compared to Bob and reducing the correlation between Alice and Eve. The effect of atmospheric turbulence will be shown in more detail in section 2.5.

In the experiment described in this thesis, the plan is to compare, for satellite to ground CV-QKD, the effect of atmospheric turbulence on the channel coherence of Alice and Bob with that of Alice and Eve. The emulation of a satellite to ground CV-QKD (down-link) was chosen for this experiment, as the atmosphere will have less of an effect compared to its up-link counterpart. Comparison of up- and down-links can be seen in section 2.4.2. In this experiment Eve is assumed to be passive at the same ground level as Bob, with Bob at the beam centre and Eve taking measurements in the surrounding areas of the beam. This means Eve is not performing any active attacks on either Alice or Bob but is passively taking measurements. This was done by emulating satellite CV-QKD and measuring the correlation between Alice's and Bob's measurements and comparing these with correlation between Alice's and Eve's measurements. The emulation was done in the lab with the atmospheric turbulence emulated using a deformable mirror. First the experiment was done with increasing turbulence with both Bob and Eve at the centre of the beam, then with Eve displaced from the centre. If Eve's measurements are less correlated compared to Bob's, then Eve has less information on the key due to the atmospheric turbulence effect. As seen in equation 1.1, with Eve having less information the signal power can be increased safely and thereby the mutual information between Alice and Bob is increased. This will increase the maximum key rate achievable. With increased key rate the channel distance can also be expanded. Although the estimation of key rate is not within the scope of this experiment, the results from this experiment can be used in future work to increase the key rate.

Chapter 2

Theory

In this chapter the background theory of QKD will be discussed and presented, with a focus on CV-QKD and satellite CV-QKD in particular. This chapter also shows how atmospheric turbulence affects CV-QKD in a free space channel and how this turbulence can be emulated. First the different quantum optical states will be presented.

2.1 Quantum Optical States

There are many quantum optical states, including fock and coherent states. Coherent states are a common state used in CV-QKD. Both fock and coherent states will be defined in this section.

2.1.1 Fock States

Fock states, also known as number states, are quantum mechanical states. Each mode of the electromagnetic field can be thought of as a harmonic oscillator, then each field mode is clearly an infinite-dimensional system (Cooper et al., 2013; Wang et al., 2008). This can then be described in terms of the usual number of fock state basis or the over-complete coherent state basis. Fock states are a multi-particle state of non-interacting identical particles. The state can be written as the sum of tensor products of N one-particle states. If the number of particles is variable, then the fock space is constructed as a direct sum of tensor products of the Hilbert space for each particle. Each mode of the electromagnetic field, characterised by the k-vector and polarisation, behaves as a harmonic oscillator. The fock states $|\mu_k\rangle$ are the harmonic oscillator Hamiltonian eigenstates and form a complete basis for each mode. The corresponding eigenvalue gives the number particle in the state. To define this as a fock state, the selected phase factor must be added. Elements of fock space which are a superposition of the states of a differing particle number are not fock states. The harmonic oscillator Hamiltonian eigenvalues for a single mode with angular frequency ω_k are (Walls and Milburn, 2007)

$$h\omega_k(\mu_k + \frac{1}{2}), \tag{2.1}$$

where μ_k is an integer, h is the Planck constant and ω_k is the angular frequency. The eigenstates are written as $\mid \mu_k\rangle$ and are known as fock states. With the eigenstates of the Number-operator $\hat{N}_k|\mu_k\rangle = \mu_k|\mu_k\rangle$:

$$\hat{a}_k^\dagger \hat{a}_k \mid \mu_k\rangle = \mu_k \mid \mu_k\rangle. \tag{2.2}$$

The vacuum state of the field mode $\hat{a}_k \mid 0\rangle = 0$, the Energy of the ground state of all the modes is

$$\langle 0 \mid H \mid 0\rangle = \frac{1}{2}\sum_k \hbar\omega_k. \tag{2.3}$$

This is infinite, since there is no upper bound to frequencies. $\hat{a}$ and $\hat{a}^\dagger$ represent the annihilation and creation of photons with the wavevector $\overrightarrow{k}$ and polarisation $\hat{e}$. They are called the creation and annihilation operators. On the fock states they are:

$$\hat{a}_k \mid \mu_k\rangle = \mu_k^{\frac{1}{2}} \mid \mu_k - 1\rangle, \tag{2.4}$$

$$\hat{a}_k^\dagger \mid \mu_k\rangle = (\mu_k + 1)^{\frac{1}{2}} \mid \mu_k + 1\rangle. \tag{2.5}$$

The number operator can be defined in terms of the annihilation and creation operators as $\hat{N}_k = \hat{a}_k^\dagger \hat{a}_k$. Now, the normalised state vectors of higher excited states can be obtained with successive application of the creation operator.

$$\mid \mu_k\rangle = \frac{(\hat{a}_k^\dagger)^{\mu_k}}{\sqrt{\mu_k!}} \mid 0\rangle \tag{2.6}$$

$$\mu_k = 0, 1, 2, ... \tag{2.7}$$

Fock states are orthogonal and complete (Gerry, Knight, and Knight, 2005).

$$\langle \mu_k \mid \nu_k\rangle = \delta_{\mu\nu}, \tag{2.8}$$

$$\sum_{\mu_k=0}^{\infty} \mid \mu_k\rangle\langle\mu_k \mid = \mathbf{I}, \tag{2.9}$$

where $\mathbf{I}$ is know as the identity operator. The norm of the eigenvectors are finite, they form a complete set of basis vectors in Hilbert space. For these reasons fock states are useful to represent high energy photons where the number of photons is small and are also a useful basis in which to expand a coherent state. From here on wards, the subscript denoting the k-vector will be drop from the notation.

2.1.2 Coherent States

Coherent states are a specific state of a quantum harmonic oscillator, with its dynamics most closely related to a classical harmonic oscillator (Walls and Milburn, 2007). They arise from quantum theory of a wide range of physical systems, and they describe the state in a system for which the minimum uncertainty ground-state wave packet is displaced from the origin of a system. These states are expressed as eigenvectors of the lowering operator and they form an over-complete family. Standard coherent states are also Gaussian states. A state is Gaussian if, the distribution function in phase space or density operator in fock space is in the Gaussian form (Wang et al., 2007)

In quantum optics coherent states refer to the quantized electromagnetic field that describes the maximum kind of coherence and are the quantum states of a field

mode that most closely resemble the classical coherent states in that mode (Zhang, Gilmore, et al., 1990). It is the minimum uncertainty state with a single free complex parameter α chosen to make the relative dispersion equal for position and momentum so they are equally small at high energy. The time evaluation is concentrated along classical trajectories of the electric and magnetic fields for that mode and the energy eigenstates of linear harmonic oscillators are fixed-numbers quantum states. The energy eigenstates of a mode are the fock states. Therefore, coherent are a superposition of fock states, which is why their photon number is uncertain.

Coherent states are defined by displacing the vacuum of a given mode. The displacement operator can $\hat{D}$ can therefore be used to define the coherent states. The displacement operator is defined as (De Oliveira et al., 1990; Král, 1990)

$$\hat{D}(\alpha) = \exp(\alpha\hat{a}^\dagger - \alpha^*\hat{a}), \tag{2.10}$$

with the coherent states being:

$$\mid \alpha\rangle = \hat{D}(\alpha) \mid 0\rangle. \tag{2.11}$$

The coherent state remains a coherent state under free field evolution and under loss with a decreasing amplitude $|\alpha|$, meaning its shape does not change with time and follows the motion of classical point particle in harmonic oscillator potential. The electromagnetic field contains an infinite number of modes, but only one is considered in the channel for information. The coherent state in terms of fock state $\mid \mu\rangle$,

$$\mid \alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum \frac{\alpha^\mu}{\sqrt{\mu!}} \mid \mu\rangle. \tag{2.12}$$

For CV-QKD the signal is sent as a series of overlapping coherent states, $\mid \alpha\rangle$ and $\mid \beta\rangle$ with their overlap $\langle\alpha|\beta\rangle$. Here unity is achieved if $\mid \alpha\rangle = \mid \beta\rangle$ and tends to zero if $\mid \alpha\rangle$ and $\mid \beta\rangle$ move apart. Therefore the amplitudes of these parameters must be small in order for these states to somewhat overlap, but simultaneously still be distinguishable by measurement. If $\beta = \alpha + \epsilon$, where ϵ is a very small parameter, the intensity $|\alpha|^2$ can also be very large and the states will still overlap. This is a necessity for CV-QKD. The quadratures of the field mode of interest are the $\hat{X}$ and $\hat{P}$ quadratures, these are dimensionless electric and magnetic fields for this mode. These can be defined in terms of the annihilation and creation operators, $\hat{a}$ and $\hat{a}^\dagger$ respectively (Gerry, Knight, and Knight, 2005).

$$\hat{X} = \frac{1}{2}(\hat{a} + \hat{a}^\dagger), \tag{2.13}$$

$$\hat{P} = \frac{1}{2i}(\hat{a} - \hat{a}^\dagger). \tag{2.14}$$

These quadratures are defined here as dimensionless and they fulfill the commutation relation.

$$[\hat{X}, \hat{P}] = \frac{i}{2} \tag{2.15}$$

In CV-QKD the quadratures of coherent states can be used to encode the information sent by Alice. The section below describes how Bob can detect these coherent states.

2.2 Detection of Coherent States

There are two methods of extracting information encoded as modulation of phase and amplitude of an oscillation signal, homodyne and heterodyne detectors (Voss, 2009; Gerrits, Glancy, and Nam, 2011). Heterodyne detectors can measure both quadratures simultaneously. A heterodyne detector is built using a beamsplitter and two separate homodyne systems. homodyne signifies a single frequency and can only measure one parameter at a given time.

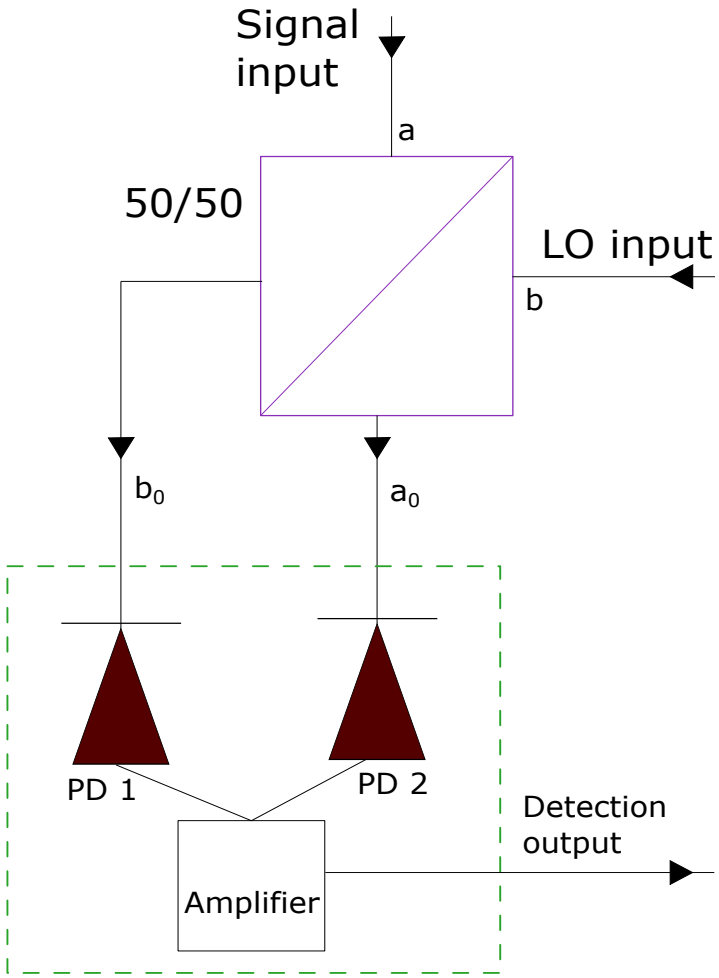

FIGURE 2.1: Set up of a homodyne detector. Here a 50/50 beamsplitter is used to superimpose the LO and signal, where 50/50 refers to the splitting ratio of the beamsplitter. PD 1 and PD 2 are the high quantum efficiency photodiodes in the detector used to monitor the two outputs of the beamsplitter. Here a and b indicate modes a and b of the detector. a_0 and b_0 are modes a and b after the transformation of the 50/50 beamsplitter.

In a homodyne detector, shown in figure 2.1, a LO with large amplitude and a weak quantum signal are superimposed using a 50/50 beamsplitter. The output of each of the beamsplitter ports are then measured by high quantum efficiency photodiodes (PDs) respectively. The individual output signals measured at these PDs are then subtracted and the difference in the signals is recorded. Therefore, in a homodyne detector from mode a and b (see figure 2.1) (Garrison and Chiao, 2008; Ficek and Wahiddin, 2014; Gerry, Knight, and Knight, 2005),

$$a_0^\dagger = Ua^\dagger U^\dagger = \frac{1}{\sqrt{2}}(a^\dagger + b^\dagger), \tag{2.16}$$

$$b_0^\dagger = Ub^\dagger U^\dagger = \frac{1}{\sqrt{2}}(b^\dagger - a^\dagger), \tag{2.17}$$

where U is the 50/50 beamsplitter transformation, a_0 is the a mode after the action of U and b_0 is the b mode after the action of U. This can also be written as:

$$a_0^\dagger = \frac{1}{\sqrt{2}}(a^\dagger + b^\dagger), \tag{2.18}$$

$$b_0^\dagger = \frac{1}{\sqrt{2}}(b^\dagger - a^\dagger), \tag{2.19}$$

$$b^\dagger = \frac{1}{\sqrt{2}}(a_0^\dagger + b_0^\dagger), \tag{2.20}$$

$$a^\dagger = \frac{1}{\sqrt{2}}(a_0^\dagger - b_0^\dagger). \tag{2.21}$$

The homodyne detector measures the difference of the photo-currents generated in the two detectors. This is proportional to the difference in the light intensities in the output modes a_0 and b_0, given by

$$I = a_0^\dagger a_0 - b_0^\dagger b_0 = a^\dagger b + b^\dagger a. \tag{2.22}$$

Assuming the state into mode b is a LO $|\beta e^{i\theta}\rangle$, now

$$\langle \beta e^{i\theta} | I | \beta e^{i\theta} \rangle = a^\dagger \beta e^{i\theta} + \beta e^{-i\theta} a = \sqrt{2}\beta \hat{x}_\theta \tag{2.23}$$

where,

$$\hat{x}_\theta = \frac{1}{\sqrt{2}}(a^\dagger e^{i\theta} + a e^{-i\theta}) \tag{2.24}$$

Now,

$$\langle I \rangle = \sqrt{2}\beta \langle \hat{x}_\theta \rangle. \tag{2.25}$$

In homodyne detection the difference of the two intensities at the two PDs is measured, this is the expectation value of the difference in receiver numbers. This expectation value is proportional to the amplitude of the LO and the expectation value of a given quadrature. The quadrature is determined by the phase chosen for

the LO. From equation 2.24, the $\hat{X}$ quadrature is measured if $\theta = 0°$ is chosen for the LO phase, and the $\hat{P}$ quadrature is measured if $\theta = 90°$ is chosen for the LO phase.

2.3 Shot Noise

Shot noise, is vacuum noise, and is a fundamental physical phenomenon in all coherent optical beams (Walls and Milburn, 2007). There may be additional sources of noise, i.e. from amplifiers, although they will only add to the fundamental shot noise. It exists since light and electronic current consists of quantized particles. A stream of photons create a visible spot, but the photons are emitted from the laser at random times, making these fluctuations shot noise. In detection the relevant process is random conversion of photons into photo-electrons. This leads to larger effective shot noise level when the detector is used with quantum efficiency below unity. The fluctuations in photo-current due to shot noise is:

$$(\Delta I)^2 \stackrel{def}{=} \langle (I - \langle I \rangle)^2 \propto \langle I \rangle, \tag{2.26}$$

where I is the intensity. Homodyne detection shot noise is attributed to the zero point fluctuations of a quantized electromagnetic field or the discrete nature of the photon absorption process.

2.4 Continuous Variable Quantum Key Distribution

Unlike in DV-QKD, in CV-QKD information is encoded in the continuous values of the quadratures of the coherent states (Walls and Milburn, 2007; Jouguet et al., 2013; Wang et al., 2017; Adesso, Ragy, and Lee, 2014). Coherent states and quadratures are defined in section 2.1.2. The use of the continuous variables for quantum communication and therefore quantum key distribution was first proposed by Ralph in 1999 (Ralph, 1999). In CV-QKD and as in DV-QKD the security is provided by the uncertainty principle (Reid, 2000), therefore CV-QKD schemes have in principle guaranteed minimum security comparable with DV-QKD schemes (Ralph, 2000). In order to measure the quadrature and therefore the raw key sent by Alice, homodyne or heterodyne detection is used. Where the quadratures are measured against a LO. A detailed description and comparison of the two detection types can be seen in section 2.2. The electromagnetic states sent through the quantum channel in CV-QKD are commonly Gaussian states, as they naturally occur as ground or thermal equilibrium states of any physical quantum system (Weedbrook et al., 2012). Additionally transformations associated with beam splitters and phase shifters, instruments implemented in CV-QKD, are naturally Gaussian. They map Gaussian states into Gaussian states. Therefore Gaussian states are particularly easy to prepare and control. From a mathematical perspective they are technically accessible, since they are completely described by a finite number of degrees of freedom despite their infinite-dimensional support in CV systems whose relative degrees of freedom are associated to operators with continuous spectrum, i.e. the eigenstates form a basis for infinite-dimensional Hilbert space.

2.4.1 Protocols

A CV-QKD protocol consists of the steps Alice and Bob take in order to exchange a secret key. There are many different protocols that can be implemented for CV-QKD. The two main kinds of protocol implementations: prepare and measure and entanglement based with their equivalent cases in Gaussian protocols (Diamanti and Leverrier, 2015). Of the two, prepare and measure is the simpler one since the states are only made and sent, whereas in entanglement based protocols, they additionally must generate entangled states. Since in this experiment only the characteristics of the channel due to atmospheric turbulence are relevant, non of the post processing procedures will be used. Although the atmospheric turbulence effect on the channel will also have a knock on effect on the post processing, this was not directly investigated in this experiment. The simplest of all the CV protocols is GG02, as it was the first protocol made for CV-QKD (Grosshans and Grangier, 2002a). This protocol was used for the experiment excluding its post-processing procedures.

For the coherent beam GG02 protocol the following steps are followed. Using Gaussian law Alice first chooses random numbers x_A and p_A with Variance $V_A N_0$ (Grosshans and Grangier, 2002a). Where N_0 is the shot noise variance which is calibrated beforehand and $V_A \equiv var(X_A)$ (Jouguet et al., 2012). She then sends coherent states $|x_A + ip_A\rangle$ to Bob. Using homodyne detection, Bob randomly measures either the $\hat{X}$ or $\hat{P}$ quadrature. A more detailed description of the coherent state detection can be seen in section 2.2. Now Alice and Bob can preform parameter estimation by revealing part of their data (Kumar, Qin, and Alléaume, 2015). They estimate the transmittance T of the channel and excess noise ξ. Using the following equations these parameters can be estimated.

$$\langle X_A X_B \rangle = \sqrt{\eta_B T} V_A, \tag{2.27}$$

$$var(X_B) = \eta_B T V_A + N_0 + \eta_B T \xi + v_{ele}, \tag{2.28}$$

where η_B is the Bob's transmission efficiency and v_{ele} is the electronic noise variance. These parameters are calibrated before the experiment, and $var(X_{B_0}) = N_0 + v_{ele}$. Using equations 2.27 and 2.28 the transmittance and excess noise can be estimated. Alice and Bob can then use reconciliation to transform it into a error-less bit string. This is usually done using parity based algorithms such as cascade (Grosshans and Grangier, 2002b). Information reconciliation is necessary since noise will make Alice's and Bob's quadrature values differ (Van Assche, Cardinal, and Cerf, 2004). This reconciliation protocol can be carried out over a public classical channel, i.e. an authenticated classical channel. QKD needs an initial authentication to insure Eve is not playing a person-in-the-middle attack on Alice and Bob. There are two main types of reconciliation, direct and reverse reconciliation. In direct reconciliation Bob corrects his key elements to have the same values as Alice. From above Alice knows the minimum amount of information she has to reveal. This type of reconciliation is less secure when the quantum channel efficiency falls below 50%. In reverse reconciliation Alice corrects her key elements to have the same values as Bob, i.e. the reverse process of direct reconciliation. Reverse reconciliation is the optimum for coherent state protocols when there is no excess noise in the transmission line. Reverse reconciliation is more secure as its is more difficult for Eve to control

the errors at Bob than to read Alice's modulations (Grosshans et al., 2003). In reverse reconciliation, for Alice to correct her raw data X_A to match Bobs raw data X_B.

For CV-QKD using reverse reconciliation the raw key rate ΔI can be calculated as follows (Lodewyck et al., 2007),

$$\Delta I_{key} = \Lambda I_{A,B} - \chi_{B,E}. \tag{2.29}$$

Here $I_{A,B}$ is the mutual information between Alice and Bob, $\chi_{B,E}$, know as the Holevo bound, is the shared information between Bob and Eve if reverse reconciliation was used and Λ is the reconciliation efficiency. Where,

$$I_{A,B} = \frac{1}{2}\log_2 \frac{V + \chi_{tot}}{1 + \chi_{tot}} \tag{2.30}$$

and χ_{tot} is the total noise between Alice and Bob.

$$\chi_{tot} = \chi_{line} + \frac{\chi_{hom}}{T}, \tag{2.31}$$

where T is the transmittance of the channel, $\chi_{line} = \frac{1}{T} - 1 + \epsilon$ is the noise in the channel and ϵ is the excess noise, $\chi_{hom} = \frac{1+v_e}{\eta} - 1$ is the noise added by the homodyne detector, v_e is the electronic noise of the detector and η is the efficiency of the detector. The information shared by Bob and Eve in equation 2.29 can be calculated as follows (Qu and Djordjevic, 2017),

$$\chi_{B,E} = G(\frac{\lambda_1 - 1}{2}) + G(\frac{\lambda_2 - 1}{2}) - G(\frac{\lambda_3 - 1}{2}) - G(\frac{\lambda_4 - 1}{2}), \tag{2.32}$$

where G is a function as described below:

$$G(x) = \frac{x+1}{2}\log_2(\frac{x+1}{2}) - \frac{x-1}{2}\log_2(\frac{x-1}{2}). \tag{2.33}$$

From equation 2.32, λ is a parameter and is calculated with the following equations:

$$\lambda^2_{1,2} = \frac{1}{2}(A \pm \sqrt{A^2 - 4B}), \tag{2.34}$$

$$\lambda^2_{3,4} = \frac{1}{2}(C \pm \sqrt{C^2 - 4D}). \tag{2.35}$$

Here the parameter $A = V^2(1-2T) + 2T + T^2(V + \chi_{line})^2$, $B = T^2(V\chi_{line} + 1)^2$, $C = \frac{V\sqrt{B} + T(V+\chi_{line}) + A\chi_{hom}}{T(V+\chi_{tot})}$ and $D = \sqrt{B}\frac{V+\sqrt{B}\chi_{hom}}{T(V+\chi_{tot})}$. The raw key rate ΔI_{key}, $I_{A,B}$ and $\chi_{B,E}$ are shown in figure 2.2 as a function of transmittance T and Variance $V = 10$.

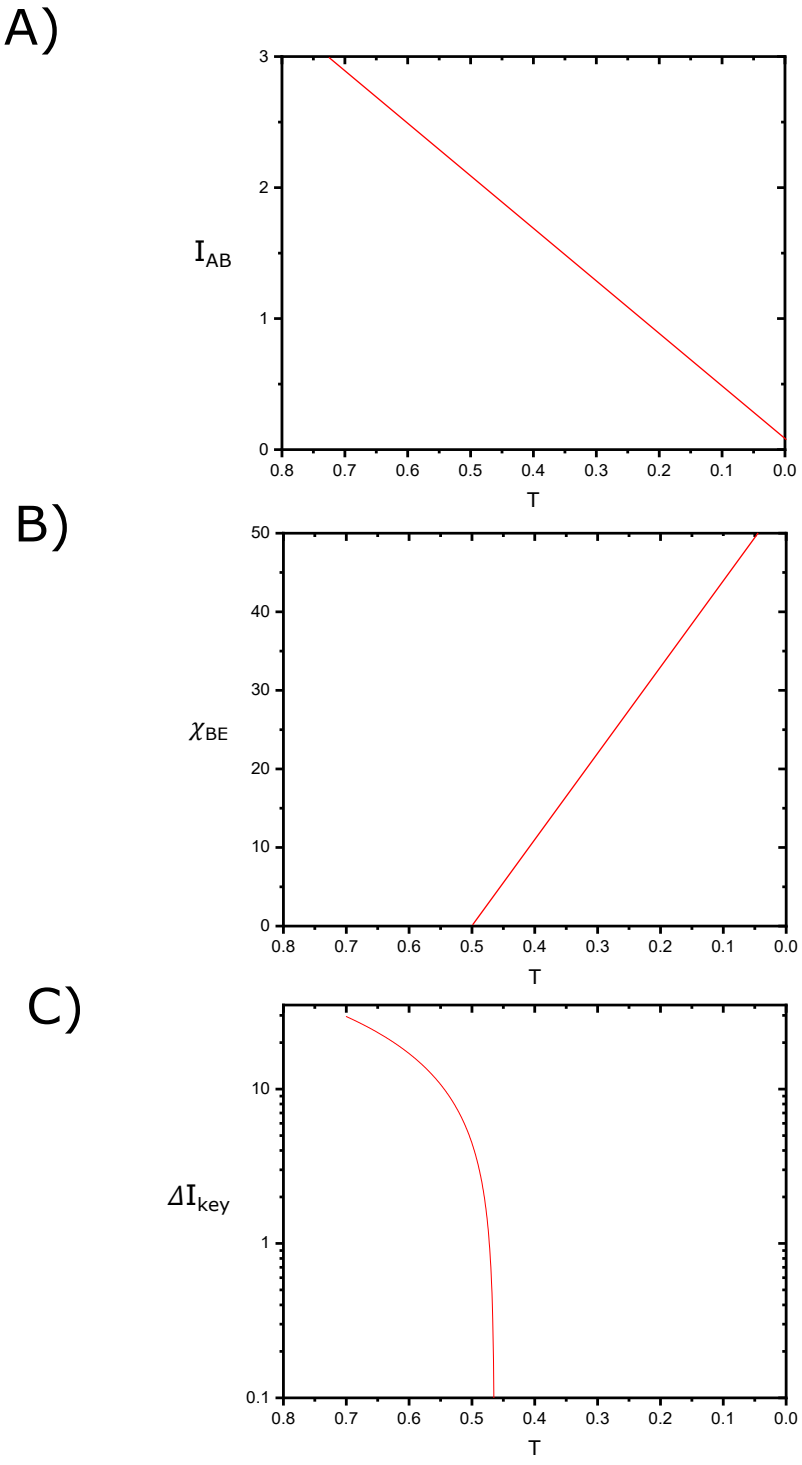

FIGURE 2.2: For A) B) and C) the variance $V = 10$, the excess noise is $\epsilon = 0.1$ and $G = 1$ A) shows how the shared information between Alice and Bob $I_{A,B}$ changes with varying transmittance T. This is calculated using 2.30 B) shows how the shared information between Bob and Eve $\chi_{B,E}$ changes with varying transmittance T. This is calculated using 2.32 C) shows how the raw key rate changes with varying transmittance T with $\Lambda = 0.95$, calculated using 2.29.

So for CV-QKD Alice sends Bob coherent states and he then measures the quadratures. Then they preform post-processing to distil the secret key. For this experiment though the relevant process is the transmission and measurement of coherent states, as this will be disturbed by atmospheric turbulence.

2.4.2 Satellite CV-QKD

The implementation of Satellite QKD is of great importance in quantum communication, as it increases the geographical coverage of the key distribution (Wang et al., 2018a), due to the non cloning theorem (Liao et al., 2017) which states that a quantum signal cannot be noiselessly amplified. This puts a constraint on how far QKD can be performed in fibre and free space. The maximum distance therefore is a few hundred kilometres. An important noise to consider in free space quantum communication, compared to its fibre based counter parts, is the noise due to the atmospheric turbulence effect. In Satellite QKD the thickness of the atmosphere is constant, thereby the communication distance can be increased. The vacuum of space does not affect the amount of noise in the channel here. Although the thickness of the atmosphere that must be traversed does depend on the zenith angle of the satellite and ground station (Tomaello et al., 2011). Though a satellite cannot be place an arbitrary distance away from the ground station, as there will also be losses due to beam divergence given a certain detector size. In 2017 a Chinese satellite verified DV-QKD at 1200km, the longest distance at the time, with a down-link (Liao et al., 2017). The downside of satellite CV-QKD is due to the LO. Here the LO must be sent from Alice to Bob. This can cause LO transmission issues as its photons may scatter and can contaminate the signal (Wang et al., 2018b). The transmitted LO (TLO) system is the easiest free space LO system to implement and mode matching is ideal at the receiver since a TLO guarantees that the spatial modes of the LO and signal are identical (Pirandola, 2021). This transmitted LO may also be controlled and modified by Eve resulting in security issues (Qi et al., 2015), due to its classical nature. Attacks on the TLO include: equal amplitude attacks, wavelength attacks and calibration attacks (Kish et al., 2021). Although there has been research into developing a Local LO (LLO) at the ground station to circumvent the problems of a TLO (Qi et al., 2015; Kish et al., 2020). This has some technical issues as the signal as LO must be perfectly timed to accomplish homodyne or heterodyne detection. In conventional LLO scheme Alice will send a phase reference pules alongside her signal in order for Bob to be able to synchronise his LLO to (Shao et al., 2021). Though since this reference pulse is a classical signal, it will also be vulnerable to attacks by a non-passive Eve.

There are two methods of constructing a satellite to ground quantum communication: up-links and down-links (Tomaello et al., 2011). In an up-link, Alice is at the ground station sending a signal to Bob at the satellite. Contrastingly, in a down-link Alice is at the satellite and sends the signal to Bob at the ground station. Here the comparative noise in these links is mostly due to beam wandering, if the dimension is large compared to the beam size, and beam broadening, although this noise can be reduced with good SNR, as it reduces link attenuation and background noise. Since Alice sends weak coherent signals with low mean photon numbers, an increased signal power cannot be used to improved SNR (Bonato et al., 2009). In satellite quantum communication down-links are the convention since the turbulent eddies that create beam spreading then appear much smaller than beam diameter and therefore the beam spreading is less strong compared to an up-link. Down-links

can also utilise a larger detector diameter on the ground than up-links could use on a satellite. Therefore it is common practice to use down-links in CV-QKD.

2.5 Atmospheric Turbulence

CV-QKD through a free space channel will be affected by the atmospheric turbulence in this channel. It is therefore of great importance to understand how atmospheric turbulence affects CV-QKD, and in order to emulate free space CV-QKD in the laboratory, how atmospheric turbulence can be modeled.

2.5.1 Zernike Polynomials

Zernike polynomials can be used to model wave distortions of a beam traveling through a turbulent medium. For this section (Arteaga-Díaz, Ocampos-Guillén, and Fernandez, 2019) was used to derive the use of Zernike polynomials as a model for atmospheric turbulence. The wavefront distortion due to atmospheric turbulence implies wave front tilt, this is the change in angle at arrival of the beam. This will then generate a phase difference $\Delta\phi$.

$$k\Delta l = \Delta\phi \tag{2.36}$$

Here Δl is the path difference and k is the wavenumber. Assuming the wavefront tilte, β_α, is small and $\langle\beta_\alpha\rangle = 0$, then the variance of the arrival angle is:

$$\langle\beta_\alpha^2\rangle = \frac{\langle\Delta\phi^2\rangle}{(kD)^2}, \tag{2.37}$$

where D the aperture diameter of the optical system. Now the phase structure of the function can be determined as

$$D_\phi(D, L) = (kD)^2\langle\beta_\alpha^2\rangle, \tag{2.38}$$

where L is the link distance. Under Kolomogorov spectral density approximation D is in the range of $\sqrt{\frac{L}{k}} \ll D \ll L_0$, where L_0 is the outer scale of the turbulent eddie. Then,

$$D_\phi(D, L) = 2.91C_n^2k^2D^{\frac{5}{3}}, \tag{2.39}$$

$$\langle\beta_\alpha^2\rangle = 2.91C_n^2LD^{-\frac{1}{3}}. \tag{2.40}$$

Now the wavefront distortion,$\phi(r, \theta)$, expressed as a sum of distortions. These can be modeled by Zerniker polynomials as

$$\phi(r, \theta) = \sum_{i=1}^{\infty} a_i Z_i(r/R, \theta), \tag{2.41}$$

which is also known as the wavenumber spectrum of the index of refraction. Where Z_i are the Zernike polynomials, R is circular aperture radius of the wavefront and a_i the weight of each of these polynomials. And a_i is given by (Noll, 1976)

$$a_i = (1/R^2) \int d^2 r W(r/R) \phi(r,\theta) Z_i(r/R,\theta), \tag{2.42}$$

where $W(r) = \frac{1}{\pi}$ when $r \leq 1$ and $W(r) = 0$ when $r > 1$. Some of the aberrations can be corrected the first j Zernike. The quadrature residual error σ_j^2 is defined as the phase variance of the total phase $\langle \phi^2 \rangle$ minus the phase variance of the total j corrected components

$$\sigma_j^2 = \langle \phi^2 \rangle - \sum_{i=1}^{j} \langle \mid a_i \mid \rangle = \sum_{i=j+1}^{\infty} \langle \mid a_i \mid \rangle. \tag{2.43}$$

As a dependence of aperture D and turbulence coherent lengthr r_0 it becomes

$$\sigma_j^2 = \Delta j (\frac{D}{r_0})^{\frac{5}{3}}. \tag{2.44}$$

The turbulence coherent length is a measure of the quality of optical transmission through the atmosphere with the in-homogeneities due to change in refractive index of the atmosphere (Zhan, Wijerathna, and Voelz, 2020). Now Zernike polynomials can be used to calculate the wave front distortion and quadrature residual error using equation 2.41 and 2.44 respectively. To emulate atmospheric turbulence using Zernike polynomials, the wavefront distortion is emulated, i.e. this is done using equation 2.41. Here the smaller order Zernike polynomials have a larger effect on the distortion as they have a larger weighting (a_i is larger with a smaller index i).

2.5.2 Turbulence Effect on Quantum key distribution

Atmospheric turbulence creates a myriad of issues for free space quantum communication. These include temporal broadening, beam extinction and extra phase noise (Wang et al., 2018a). Beam extinction causes transmittance fluctuations, due to absorption and scattering by molecules and aerosols. The added phase noise arises due to the random variation of the index of refraction of the atoms (Fante, 1975), which adds extra phase to the signal. This change in refractive index is caused by temperature fluctuations in the Atmosphere. These temperature fluctuations create turbulent eddies, which change the refractive index (Popoola et al., 2009).

The primary cause of performance deterioration on free space quantum communication is due to transmittance fluctuations caused by beam wandering, beam broadening beam wavefront deformation and scintillation. If a TLO is used for CV-QKD, then the LO will encounter the same issues due to turbulence as the signal does. This is a large disadvantage a TLO has compared to a LO that is generated locally by Bob at a ground station (LLO), although LLOs have their own draw backs on practical implementations such as phase drift caused by a de-synchronised laser (Kish et al., 2020). This arises since the laser and LLO are not phased locked.

2.5.3 Modelling

Electromagnetic propagation through a turbulent media requires many different models to describe all the effects experienced by the propagating beam. The electromagnetic wave propagation for example can be modeled using the Markov approximation. In this experiment, the relevant measurements taken are to compare the difference correlation between Alice and Bob against the correlation between Alice and Eve, at different parts of the beam due the atmospheric turbulence effect. As seen in section 2.4.1, for coherent state CV-QKD, overlapping states $|x + ip\rangle$ are sent from Alice through the free space channel to Bob. The refractive index will differ at different sections of the beam, this means the added phase noise at different sections of the beam due to the change of refractive index will change the previously mentioned correlations. Therefore, the relevant atmospheric turbulence effect for this experiment will be the fluctuations of the index of refraction as they will add phase noise. Atmospheric turbulence effects such as beam wandering and beam broadening will not be relevant. Although, these effects will have an effect on the transmittance in the channel and therefore an effect on overall key rate achievable (as seen in equations 2.29, 2.30 and 2.31), they will not change the correlations between Alice and Bob, and Alice and Eve.

There are multiple turbulence models that model the fluctuations in the index of refraction. The Index-of-refraction model models the change in the index of refraction over time (Fante, 1975). Zernike polynomials can also be used to model the index of refraction. These are significantly easier to model in the laboratory. Using a deformable mirror (DM), Zernike polynomials can be inputted to change a parallel beam to a distorted one by applying voltages to sections of the DM. These DM sections tip and tilt to deform the wavefront. Using Zernike polynomials and a DM, turbulence can now be emulated when limited to the laboratory. The turbulence used on the DM with various different Zernike polynomials can be seen in the appendix A.

The background theory and equations presented in this chapter can now be tested experimentally. Here the apparatus and experimental set up will be presented in the following chapter, chapter 3.

Chapter 3

Apparatus and Method

In this chapter the apparatus, experimental set up and experiment procedure will be presented using the background theory presented in chapter 2. First the balancing of the homodyne detector will be discussed in section 3.1, then the shot noise sensitivity will be checked in section 3.1, followed by the experimental set up in section 3.2 and lastly the experimental procedure in section 3.3.

3.1 Homodyne Detector

The homodyne detector used in the experiment must be balanced before taking any measurements, with a diagram of a homodyne detector seen in section 2.2 in figure 2.1. In a balanced homodyne detector the photo current from both PDs cancel each other out, which requires the light to arrive simultaneously at the PDs. Balancing is done by sending the LO through a 50/50 beamsplitter to the homodyne detector, with set up as seen in figure 3.1. Here the photo-currents from both PDs of the homodyne detector are balanced in such a way that the mean output signals are zero. Using a variable attenuator to add proper attenuation in one of the output ports of the 50/50 beamsplitter, will balance the homodyne detector.

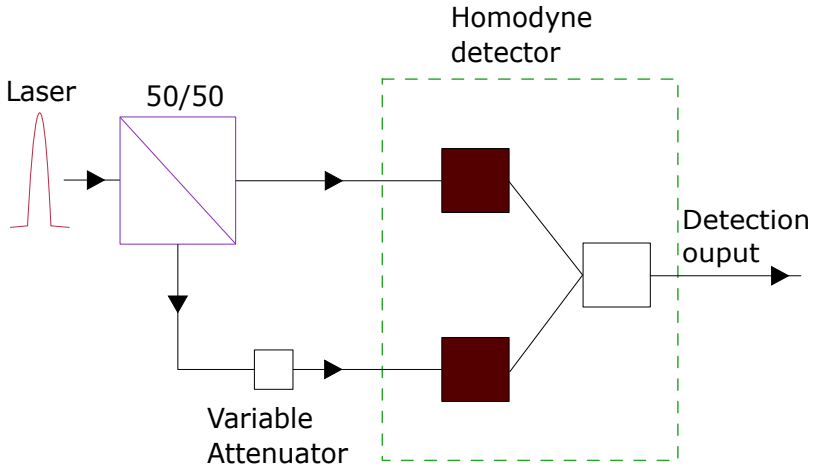

FIGURE 3.1: Experimental set up for balancing the homodyne detector. Here 50/50 refers to the splitting ratio of the beamsplitter. Polarisation maintaining fibre components were used in this set up.

In order to perform any CV-QKD experiment, first check if the homodyne detector is shot noise sensitive. This is verified by examining the linear response of the homodyne detector output variance with respect to LO intensity and finally quantifying the electronic noise variance in shot noise units. Therefore the noise of the detector is measured with regards to the LO power inputted. The LO was sent to the homodyne detector without the signal.

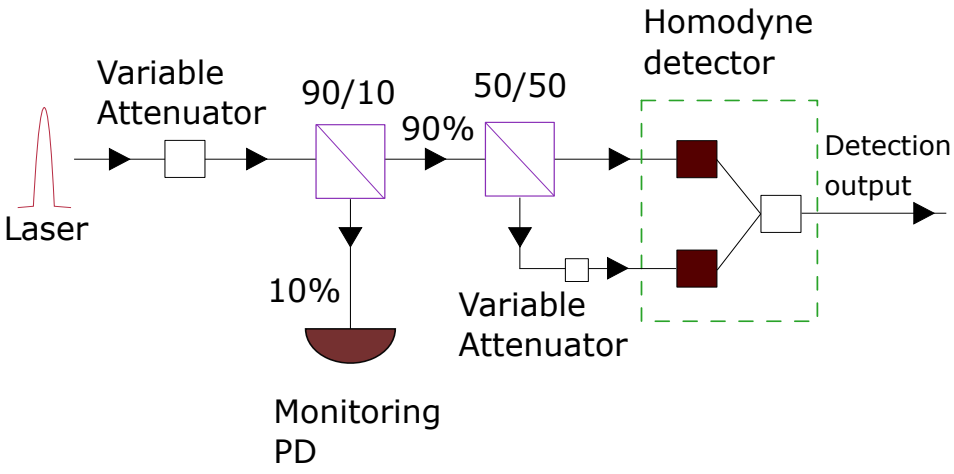

FIGURE 3.2: Set up to estimate the shot noise variance. Here 90/10 and 50/50 are the splitting ratios of the respective beamsplitters. Polarisation maintaining fibre components were used in this set up, with the photodiode (PD) in the 10% line used in order to monitor.

Figure 3.2 shows the experimental set up, but a more detailed homodyne detector can be seen in figure 2.1 of section 2.2. Here a laser with 1550nm wavelength was used with a polarisation maintaining 50/50 beamsplitter. A function generator (FG) was used to generate electrical pulses of width 82ns at 1MHz repetition rate. These were used to trigger the laser and data acquisition card (DAQ card). A DAQ card is a data acquisition device that can generate or acquire data. During this measurement it converts the analog homodyne detection data into digital values. They can also be used to send signals from a computer to other instruments in order to control these remotely from a computer. The DAQ card is clocked and synchronised with the homodyne output such that every rising edge of clock signal enables the DAQ card to read the homodyne output. Since the path for the DAQ clock is shorter than that for the laser, it must be delayed. This delay was measured by using the same set up as described above with the homodyne detector replaced with a simple photodiode. For estimating the delay, the output and DAQ clock were connected to an oscilloscope. The two distances between the peaks from the DAQ clock and photodiode outputs were measured, and thereby the delay between them. This can then be used to delay the DAQ trigger internally with the function generator, i.e. the delay is adjusted electronically and not by a transmission path. Using this setup the shot noise variance of the detector can be measured. First in order to determine the electronic

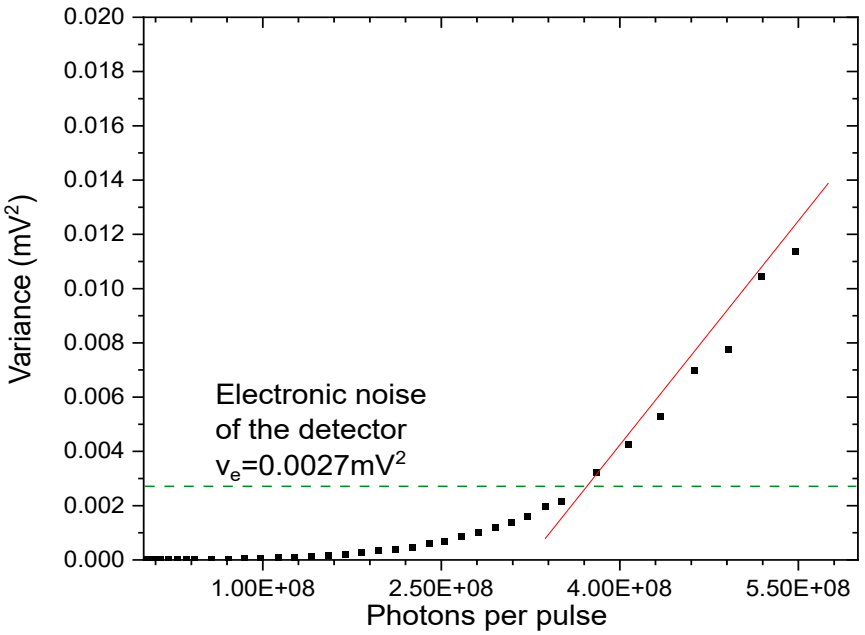

FIGURE 3.3: Linear response graph of the homodyne detector. Where the y-axis is the shot noise variance of the homodyne detector and the x-axis the photons per pulse of the LO. Here the red line indicates the linear region. Here this line was fitted to the linear region of the graph, excluding the non linear data points. The green dotted line indicates the electronic noise of the detector, which is $v_e = 0.0027mV^2$.

noise of the detector v_e, the homodyne output variance was measured without the LO signal. Then the average power of the LO was increased in increments of $0.2\mu W$. Figure 3.3 shows the results of this test. Here the graph shows the detector has a linear response with the electronic noise of the detector $v_e = 0.0027mV^2$. Therefore, the detector is shot noise sensitive in the linear region of the graph and the shot noise variance is above the threshold of the electronic noise of the detector. This graph is known as the linear response graph.

3.2 Experimental set-up

Figure 3.4 shows the experimental set up including both the free space path and Alice. Alice is built using fibre components to generate the quadratures that are sent to Bob. First the free space component will be discussed, then the fibre component. A more detailed homodyne detector diagram can be seen in figure 2.1 of section 2.2.

The free space component consists of Alice's collimator, a DM (deformable mirror) to emulate the atmospheric turbulence effect and Bob and Eve's receiver, where the signal travels from Alice's collimator to the DM and then to Bob and Eve's receiver. The receiver then outputs the signal through fibre into the 50/50 beamsplitter for homodyne detection. The receiver in this experiment is shared by Bob and Eve, and attached to a translation stage. Here Bob is considered to be at the centre of the beam, while Eve is displaced from the centre. Therefore, the experiment was first run were the receiver is considered to be Bob. It was then repeated with the receiver considered to be Eve, but using the translation stage to displace the receiver from

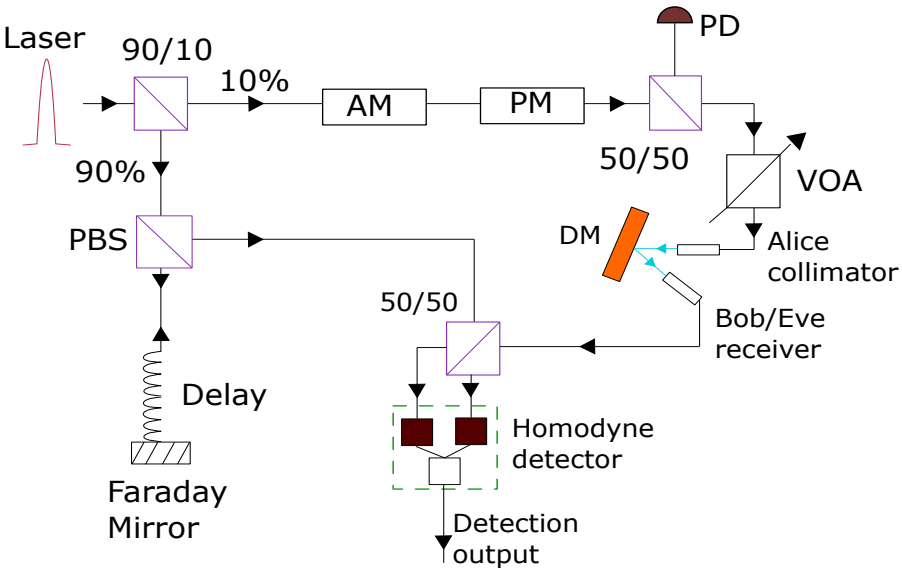

FIGURE 3.4: Complete experimental set up, including fibre and free space components. Here 90/10 and 50/50 refers to the splitting ratio of the beamsplitts. Both these are polarisation maintaining. Where PBS is a polarising Beamsplitter, AM the amplitude modulator, PM the phase modulator, VOA the variable optical attenuatetor. The photodiode (PD) is used to monitor. The blue lines refer to the beam propagation path in free space. Here a deformable mirror (DM) is in the free space path.

the centre of the beam.

Here the atmospheric turbulence is emulated using a DM from Thorlabs (DMP40/M-P01). The DM is a sectioned mirror that makes a parallel wavefront into a distorted one by applying different voltages to the sections of the DM. These applied voltages deform the sections of the DM and therefore these mirrors create tips and tilt to deform the wavfront. The DM sections can be manipulated with the different Zernike polynomials that display various kinds of turbulence as shown in section 2.5.1. This is done using the deformable mirror software package provided by Thorlabs. Therefore, the DM can emulate the atmospheric turbulence effect of large propagation paths for satellite to ground CV-QKD in the laboratory with small propagation paths.

For the fibre component of this experiment the laser is split into two lines in order to generate both the LO and the signal, as shown in figure 3.4. A 90/10 beamsplitter was used, since in CV-QKD the signal power must be small comparatively to the LO. The signal line then continues to an amplitude modulator (AM) and phase modulator (PM), both controlled by Alice's PC. An additional 50/50 beamsplitter was added for monitoring purposes. From there, the signal line continues to a variable optical attenuator (VOA) which controls the signal power output. From there the signal line is connected to Alice's collimator and sent through the free space. The laser pulse 90% line seen in figure 3.4, is the LO. Since the signal path is much longer than that of the LO, the LO was delayed. This was done using a polarizing beamsplitter (PBS) and Faraday mirror (FM), where the LO signal first passes through the PBS and is

sent to the FM and back to the PBS before entering the 50/50 beamsplitter at the homodyne detector. For the correct delay, the fibre path between the FM and PBS must be at such a length that the LO and signal both reach the homodyne detector simultaneously.

All the fibre mentioned above was polarization maintaining fibre in order to preserve the polarisation of the signal or LO. All the fibre connections were uniform using FC/APC connectors throughout.

3.3 Experimental Procedure

For this experiment a GG02 protocol, excluding its post processing procedures as mentioned in section 2.4.1, was used. Here Alice prepares and sends Bob coherent states and Bob measures these using a homodyne detection. No post processing was done for this experiment, as the relevant measurements are to compare the correlations between Alice and Bob with the correlation between Alice and Eve. The theory of coherent states can be seen in section 2.1.2 and homodyne detection in section 2.2. In order to run the experiment, first the delay in the LO path must be estimated and added to the system. This process can be seen in section 3.3.1. The data acquisition must also be added to the system, this can be seen in section 3.3.2

3.3.1 Estimation of Delay

The delay is built using a PBS, fibre and a Faraday mirror (FM), where the fibre refers to delay in figure 3.4. Here the PBS and FM can be used to make a delay by utilising the polarisation multiplexing properties of the PBS and the polarisation rotating properties of the FM. Figure 3.5 shows the polarisation multiplexing of the PBS. Here the PBS lets one polarisation pass to the slow axis output through the slow axis of common port whilst the second polarisation, which is 90° rotated compared to the first polarisation, routes to the fast axis output of the PBS through the fast axis of the common port. The FM is a mirror where the light reflected off of it is rotated by 90°, this is due to Faraday rotation. Faraday rotation or Faraday effect causes polarisation rotation (Schatz and McCaffery, 1969). This rotation is proportional to the magnetic field along the light propagation path. Using the PBS and FM properties, a delay can be built, as shown in figure 3.5. Since in the set up of this experiment LO line uses polarisation maintaining fibre (as seen in figure 3.4), the input polarisation of the light into the PBS is uniform along the slow axis of the fibre. Now the light routes in the PBS along the slow axis to the FM. The polarisation of the light is the rotated 90° and is reflected back along the fast axis to the output. This increases the path of the LO light and thereby making a delay line. Additional fibre can be placed in between the PBS and FM to increase the propagation path and, therefore, the delay of the LO.

In order to build the delay, first the amount of delay on the LO must be measured. Here the difference in arrival times of the LO and signal at the homodyne detector were compared. This was done by using the complete experimental set up described above in section 3.2. A FG was used to trigger the $1550nm$ laser pulsed with a frequency of $1MHz$ and a pulse width of $82ns$, this was a classical signal. Instead of using a homodyne detector to take the measurements, a photodiode connected to an

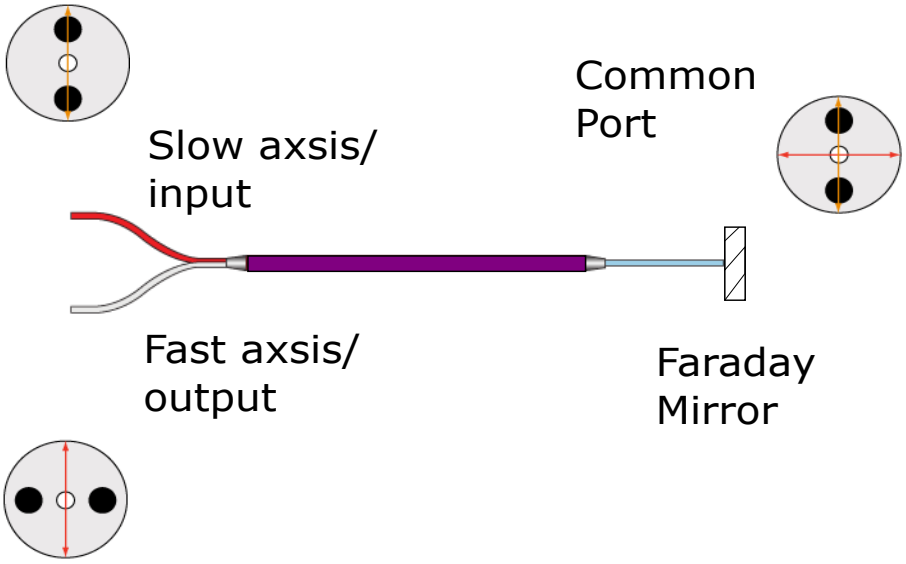

FIGURE 3.5: The multiplexing of a PBS. Here cross sections of the fibre are shown for all input and output ports. The yellow arrows represent the polarisation along the slow axis and the red arrow the polarisation along the fast axis. This figure shows how a PBS and FM can be used to make a delay. With the input light passing through the slow axis of the PBS to the FM where it is reflected back with 90° added to it. It then passes through the fast axis of PBS to the output and transmitted to the homodyne detector.

oscilloscope was used. In order for the signal peak to be visible at this oscilloscope the lines at the 90/10 beamsplitter must be switched. This means instead of sending 90% of the laser light through the LO line, now this 90% goes through the signal line. This was necessary since the signal line is much more lossy and if only 10% of the laser light is used, then it is not possible to determine the location of the pulse peak at the oscilloscope. Now the location of the signal pulse peak and LO pulse peak were determined, by only having one line connected at a time. First the LO line was disconnected and the location of the signal pulse peak was measured, then the same was done for LO. The difference in these locations is the required delay for the LO line. This delay in nanoseconds can be converted to length in fibre using delay in $\frac{ns}{4.99} = \textit{fibre length in metres}$. Only half the amount of fibre length is required to build the delay since a FM is used and the light must therefore pass through the same fibre delay twice before exiting to the detector. Now the delay was tested, by adding the delay to the system. Both the lines were connected to the output. If the delay is the perfect length these two signals will interfere and show constructive and destructive interference with respect to their relative phase. If this is the case, then live splicing is undertaken.

Here a section of fibre in the delay line was cut. Using the fibre splicer to align the two cut and exposed sections of the delay line to continuously test the delay as shown in figure 3.6. Now small pieces of the fibre were cut before the delay was retested. This was done until the two signals start to show interference. The figure 3.7 shows how the two signals interfere before they are aligned properly. As the signals approach this, first many peaks are visible at the oscilloscope, then fewer beating peaks, until no peaks are visible and the signal oscillates between the interference maximum and minimum. This is due to the change in relative phase of the two pulses that are interfering.

Here a nanosecond of accuracy is required. This is due to the laser being chirped. In a chirped pulse, each pulse of the laser the charges are accelerated (Strickland and Morou, 1985). Therefore without nanosecond accuracy, the incoming pulses from both outputs of the 50/50 beamsplitter would effectively superimpose differing frequencies, due to the chirp, and multiple peak arise, as seen in figure 3.7. The only condition when the same frequency is superimposed across the overlap of the two pluses is when the delay is within this nanosecond accuracy.

3.3.2 Data Acquisition

There are two triggers required for the data acquisition of this experiment, one trigger for Alice to modulate the signal (the writing trigger) and one for Bob/Eve to read the measurements (the reading trigger). Figure 3.8 shows the set up of these triggers with the DAQ card.

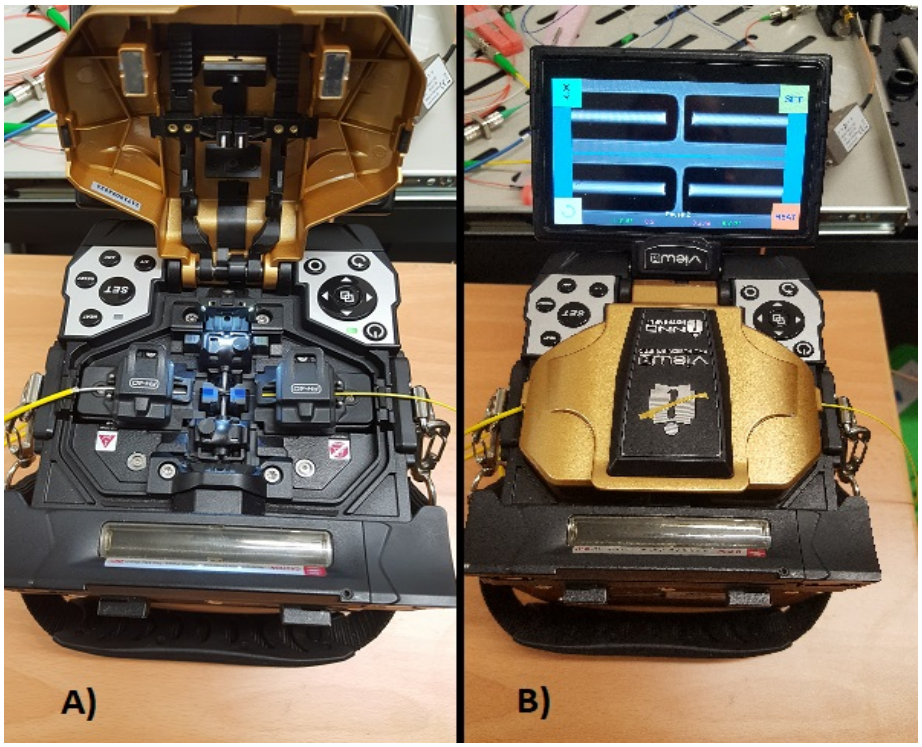

FIGURE 3.6: Fibre splice used to splice fibre as well as live splicing. A) is interior of the splicer with to two ends of fibre, that will be spliced, inserted in it. B) is the exterior of the splicer with to two ends of fibre, that will be spliced, inserted in it. The display shows how well aligned theses these fibre ends are.

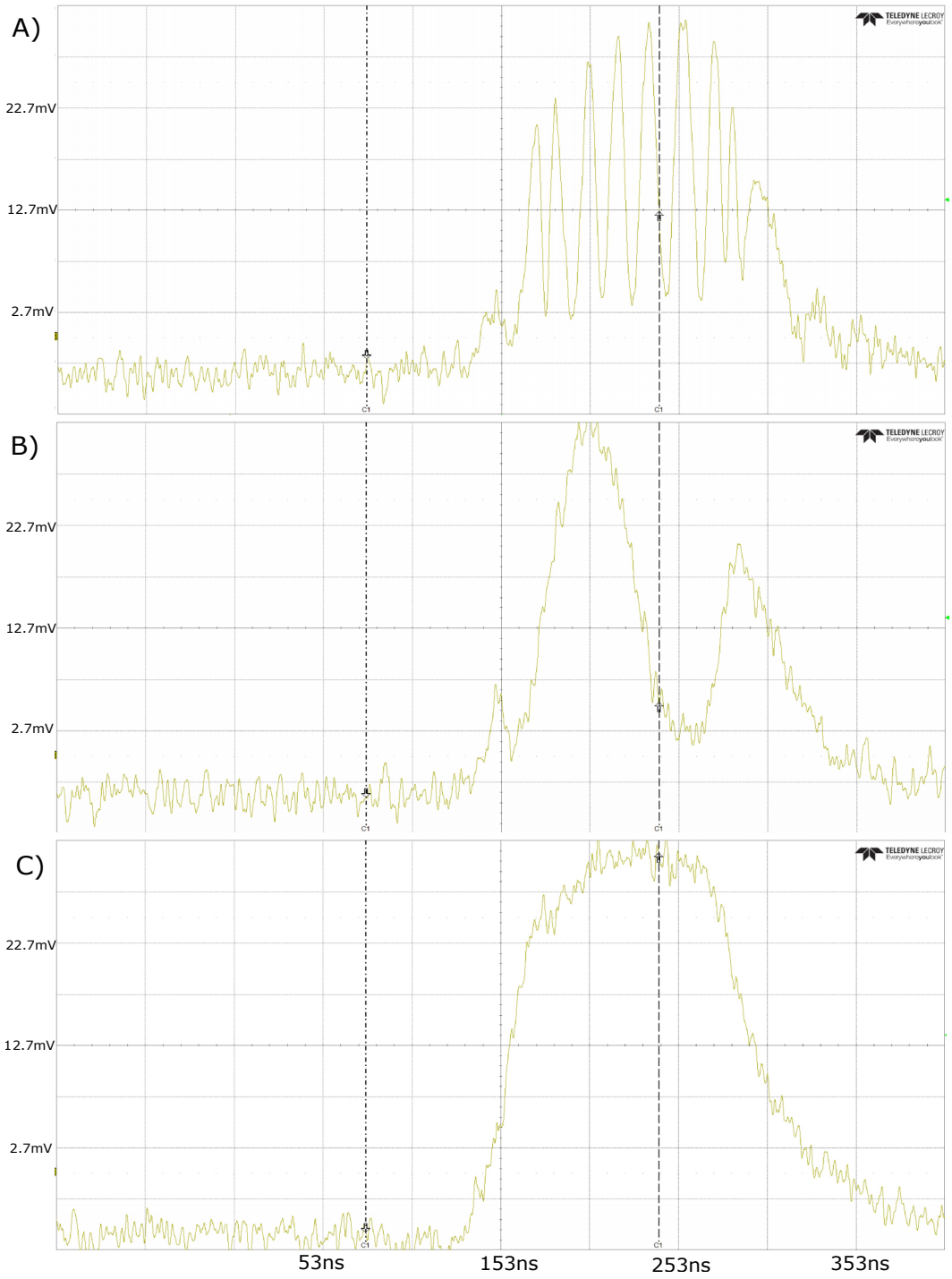

FIGURE 3.7: Interference pattern of LO and signal line using a chirped laser, in the oscilloscope display, as the delay line approaches the length of the signal line. Here the profile shape of the graph is the relevant feature. For all graphs the y-axis the electric field and the x-axis is time. The x-axis has the same dimensions for all three graphs. A) has strong interference, as the LO line is some nanoseconds too long. B) shows fewer number of interference maxima and mimimas, as the delay approaches the correct length. C) shows only one peak as the light from LO and signal line come into the detector simultaneously. The peak here will oscillate between the interference maxima and minima due to the change in relative phase of the two pulses that are interfering

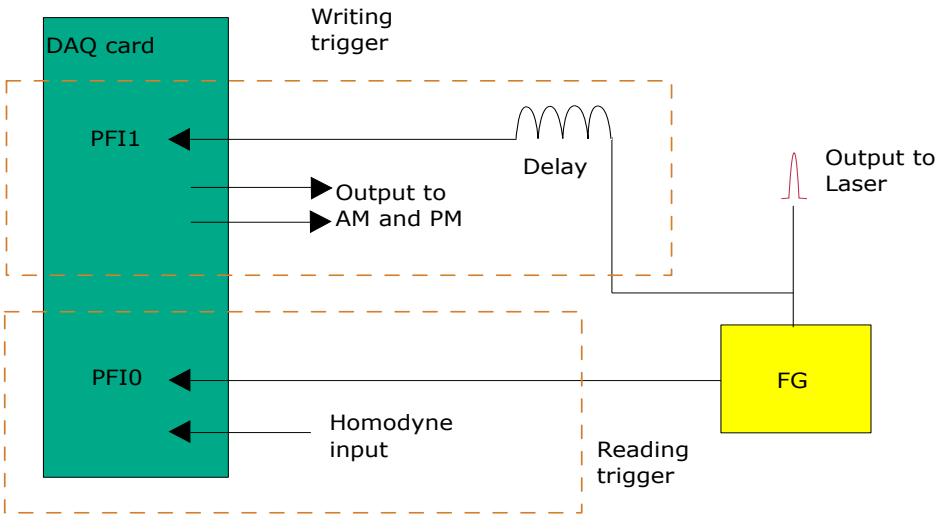

FIGURE 3.8: Trigger set up with DAQ card. Where the reading trigger is delayed internally by the Function Generator (FG) and the writing trigger is delayed externally by increasing the path length. The output of the writing trigger, trigger the modulation at the amplitude modulator (AM) and phase modulator (PM). PFI1 and PFI0 refer to the input channels at the DAQ card of the writing and reading triggers respectively

Reading Trigger

In order for Bob/Eve to read the measurements taken by the homodyne detector, a trigger is required. This trigger tells Bob/Eve when the peak of the measurements are present and for the DAQ card to read and input them into the PC. Since the path for the trigger is shorter than that for the laser, it must be delayed. The experimental set up was used, see figure 3.4, with the homodyne detector replaced with a simple photodiode. Here the output and trigger were connected to an oscilloscope. The two distances between the peaks from the trigger and photodiode output were measured and thereby the delay between them. This can then be used to delay the trigger internally by the function generator. Here the laser was triggered using a FG with a frequency of $1MHz$, pulsed with a width of $100ns$, this was also used for the trigger. The trigger was then internally delayed by the FG by $260ns$ with the rising edge of the trigger pulse used to trigger the reading.

Writing Trigger

This trigger was used by Alice. Here the trigger tells Alice when to write, i.e. when to modulate the amplitude and phase. A trigger is required for this since these modulations are only possible when a laser pulse is present in the AM for amplitude modulations and the PM for phase modulations. This means the paths for the optical signal from the laser and the electrical signal that tells the modulators to write are matched. Now the optical pulse and the command to write information into the pulse arrive at the modulators simultaneously. In figure 3.8 one of the lines out of

the FG is split, one is used to trigger the laser, the other is used to trigger the writing for the DAQ card. Here an external delay was used, i.e. the delay was increased by increasing the propagation path. To check the amount of delay, the output from the AM was connected to an oscilloscope using a photodiode. The trigger was also connected to the same oscilloscope. Here the laser was triggered as described in the above section. In order for Alice to write correctly, at the oscilloscope the laser pulse must be within the reading trigger pulse. If this is not the case, then a longer cable is required for the writing trigger. The cable length was increased until the laser pulse was within that of the writing trigger.

In order to later normalise the data taken, first the experiment was run under perfect conditions, i.e. data was taken by Bob at the centre of the beam without turbulence. This was also done with the free space component replaced by fibre of the same length to compare how the free space component affects the transmittance and, therefore, the correlation of the experiment. Then, to compare how turbulence effects the coherence of Bob vs Eve, two different methods were implemented. First, Bob and Eve were both set to be at the centre of the beam and with no differentiation made between them, as they are both considered to be at the centre of the beam. Here, both Bob and Eve took data for four different turbulence conditions. The second method implemented was by considering Bob and Eve at different parts of the beam. Here both Bob and Eve are considered to be at a ground station with Eve displaced from the centre of the beam, i.e. both Bob and Eve are on the same plane of the beam with Eve at increasing distances from Bob and the centre of the beam. Bob takes data at the centre of the beam with a given turbulence and Eve takes data with the same turbulence at a different point of the beam. This was done with three different turbulence degrees. In order to ensure Eve takes the data at the same points of the beam for each turbulence, her receiver was moved horizontally with a translation stage. She took points at $2.78mm$ and $5.56mm$ from the centre of the beam. These displacements translate to 27.8% and 55.6% of the beam radius respectively, where the beam radius for the experiment was $1cm$. All the results from this section are presented in the next chapter, chapter 4.

Here the relevant measurement is the correlation, as the experiment is to compare the information difference between what Alice prepares and sends and what Bob and Eve receive with respect to the turbulence in the channel. Therefore correlation is use full measurement for this comparison. The correlation coefficient can be used to show how related two measurements are to each other (Chen, Smithson, and Popovich, 2002; Dadson, 2017), if the coefficient equals 1, then the two measurements are perfectly correlated, i.e. the same value. If the correlation coefficient equals 0, then there is no correlation between the two measurements. And if the correlation coefficient equals -1, then the two measurements are perfectly anti-correlated, i.e. they are the inverse of each other. The correlation coefficient between two measurements x and y can be calculated as such:

$$\rho_{x,y} = \frac{cov(x,y)}{\sigma_x \sigma_y}, \tag{3.1}$$

where cov is the covariance, in terms of the expectation value $E(x)$ of x and expectation value $E(y)$ of y, the covariance is: $cov(x,y) = E(xy) - E(x)E(y)$. σ_x is the standard deviation of x and σ_y is the standard deviation of y.

3.3.3 Atmospheric Turbulence

The atmospheric turbulence emulated for the experiment was modeled using a DM from Thorlabs (DMP40/M-P01). With this particular DM, Zernike polynomials can be used to generate the wavefront distortions that arise due to turbulence, as described in Section 2.5.1. Here the Zernike polynomials Z_n were changed in order to create the different wavefront distortions. Where n refers to the specific Zernike polynomial. The smaller n is the greater affect it has on the level of turbulence generated as stated in from 2.5.1, equation 2.41. This can be seen in the wavefront distortions of the DM as shown in the Appendix A. For the first part of the experiment, where Bob and Eve are both in the centre of the beam with differing turbulence conditions, turbulence degree (t) were chosen as shown in the first column of table 3.1. Here the strength of turbulence t_n increases with larger n. For the second part of the experiment where Bob and Eve are considered to be at different parts of the beam with the same turbulence condition, the turbulence degree were chosen as shown in the second column of table 3.1. Here the degree of turbulence increases from t_a to t_c.

Turbulence name, Eve in the centre	Turbulence name, Eve displaced	Zernike Polynomials
t_1	–	$Z_7 = 1; Z_8 = 1$
t_2	t_a	$Z_5 = -0.5; Z_7 = 1$
t_3	t_b	$Z_4 = 1$
t_4	t_c	$Z_4 = 1; Z_5 = -0.5$

TABLE 3.1: Turbulence degrees chosen for Bob and Eve, without displacing Eve from the centre of the beam shown in the first column. Turbulence degrees chosen for Bob and Eve, when displacing Eve from the centre of the beam shown in the second column. The final column shows the Zernike polynomials for a given turbulence degree.

Using the apparatus and experimental procedure presented in this chapter, the measurements were taken. These results of this experiment will be presented and discussed in the following chapter, chapter 4.

Chapter 4

Results and Discussion

In this chapter the results obtained for the experiment will be presented and discussed with their implications on the satellite CV-QKD. As stated in section 3.3, the measurements taken in this experiment are correlations of Alice and Bob as well as Alice and Eve. If the correlation between Alice and Eve is less than that of Alice and Bob, then Eve has less information, and the channel is more secure. Although, in this experiment no post-processing procedures were directly analysed, the results will have a knock-on effect on them as stated in section 2.4.1.

Table 4.1 shows the results for the experiment under perfect conditions, i.e. where the free space section was replaced with fibre, and no turbulence was applied to the DM. Fibre is considered as a reference for free space. Here $\rho_{A,B}$ in fibre refers to the correlation between Alice and Bob through a fibre path, where the set up in figure 3.4 was used with the free space path replaced with fibre of the same length. $\rho_{A,B}$ in free space without turbulence refers to the correlation between Alice and Bob through free space path without turbulence in the channel, where the set up described in figure 3.4 was used. The correlation was calculated using equation 3.1, where x is the state set by Alice and y is the state measured by Bob.

$\rho_{A,B}$ in fibre	$\rho_{A,B}$ in free space without turbulence
$0.26 \pm 8 * 10^{-4}$	$0.25 \pm 8 * 10^{-4}$

TABLE 4.1: Comparative correlation between Alice and Bob for the experiment with fibre, and no turbulence applied to channel. Here the correlation is defined in equation 3.1, where the states set by Alice are x and the states measured by Bob are y.

From table 4.1, the free space path, without turbulence applied to it, only decreases the correlation between Alice and Bob by $1\% \pm 0.08\%$ compared to the same channel through fibre. This reduction in correlation is most likely due to loss in the free space channel. From equation 2.30 the mutual information between Alice and Bob, and thereby their correlation, decreases with increased total noise χ_{tot} which in turn depends on the noise of the channel χ_{line} and of the homodyne detector χ_{hom} (see equation 2.31). Since the free space path and same channel through fibre shared the same set up for Alice and Bob's detector, the correlation difference is therefore due to more noise in free space channel compared to the same channel through fibre. The channel noise $\chi_{line} = \frac{1}{T} - 1 + \epsilon$, ϵ is the excess noise and the term $\frac{1}{T} - 1$ is noise due to losses. The main losses in the free space channel compared a same channel through fibre is due to beam widening and coupling. Loss from beam widening

arises as Bob can now only measure the a section of the beam. The loss due to coupling, as Bob's receiver is in fibre, the free space channel cannot couple properly to fibre and this creates loss. Comparing the correlations in table 4.1, the majority reduction in correlation between Alice and Bob is unrelated to the different channels used, as comparative loss in correlation due the the change in channel is relatively small compared to the overall loss in correlation. This indicates there is more signal loss elsewhere in the system unrelated to the free space channel. This is a positive reflection on the use of a free space channel. The correlation $\rho_{A,B}$ in free space without turbulence seen in table 4.1 can be used to normalise the results of the experiment as stated in section 3.3. The later results can be normalised since only the comparative correlations is important for this experiment and not the absolute correlation.

4.1 Bob and Eve at the centre of the beam with varying turbulence

As described in section 3.3, first the experiment was undertaken with varying turbulence degrees for both Bob and Eve without displacing Eve from the centre of the incoming beam. Here no distinction was made between Bob and Eve as they both are considered to be at the centre of the beam and therefore, measure the same values. This was done as a reference test under ideal conditions for Bob and Eve in order to show how turbulence effects correlation in a free space channel. The initial correlation for Bob and Eve, where the correlation $\rho_{A,B/E}$ is between Alice and Bob/Eve who are considered to be the same in this scenario. The correlation was calculated using equation 3.1, where Alice is x and Bob/Eve are y. The turbulence degrees chosen here are as shown in table 3.1, where the wavefront distortion used at the DM can be seen in the Appendix A. Here the turbulence degree t_n increases with increasing index n of the turbulence degree t. This is due to the fact that smaller order Zernike polynomials have a greater contribution to an increased turbulence effect as stated in section 2.5.1 and seen in equation 2.41. These results must then also be normalised using the $\rho_{A,B}$ in free space without turbulence in the channel as shown in the second column of table 4.1. The normalisation is done by dividing the experimental results by $\rho_{A,B}$ in free space without turbulence in the channel as shown in the second column of table 4.1. The correlation between Alice and Bob/Eve using these corrections, is shown in figure 4.1. This figure shows how the correlation $\rho_{A,B/E}$ changes as a function of turbulence degree. Here the turbulence degree increases from $t_1 - t_4$. Figure 4.1 shows a correlation reduction with increased turbulence degree.

From the results of Bob and Eve at the centre of the beam with varying turbulence degrees as shown in figure 4.1, the correlation is reduced when the turbulence degree is increased. The correlation reduction with increased turbulence degree is expected, as increased turbulence degree increases the noise of the channel. This is due to the change in refractive index, beam widening, scattering etc. As stated in section 2.5.3, the relevant effect for CV-QKD is the change in refractive index due to atmospheric turbulence. Which can be emulated using a DM. These turbulence effects reduce the transmittance of the channel as described in section 2.5.2 and (Hosseinidehaj et al., 2018; Wang et al., 2021). The information shared between Alice and Bob, $I_{A,B}$ depends on this transmittance, as seen in equations 2.30 and 2.31. Therefore, the correlation between Alice and Bob, $\rho_{A,B}$, also depends on the transmittance of the channel, as $I_{A,B}$ and $\rho_{A,B}$ are related in a monotonically increasing manner.

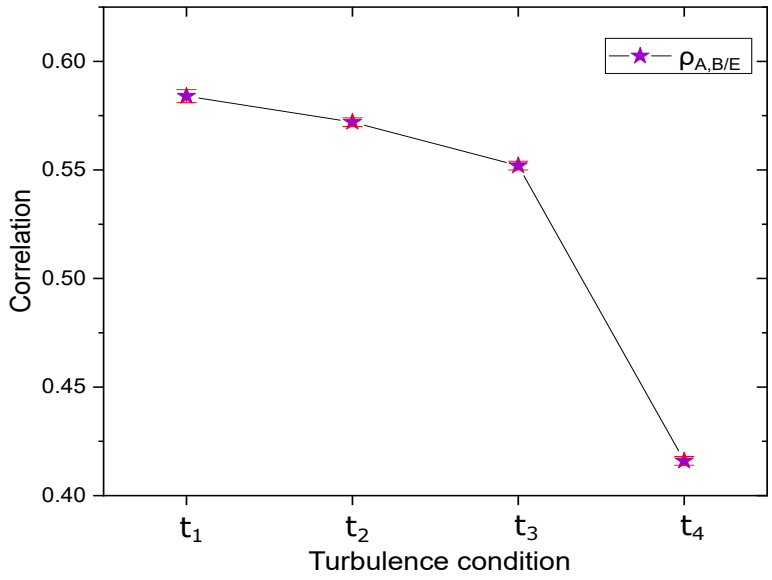

FIGURE 4.1: Normalised correlation results $\rho_{A,B/E}$, with Bob and Eve at the centre of the beam and varying turbulence degrees. Here there is no distinction made between Bob and Eve as they are both at the centre of the beam and therefore have the same results. The correlation $\rho_{A,B/E}$ refers to that between Alice and Bob/Eve and is calculated as shown in 3.1, where Alice is x and Bob/Eve are y. Where the strength of turbulence t_n increases with larger n and the error is shown in red. Here the x-axis is not necessarily linear.

This shows the results in section 4.1 are consistent with the theory.

From equation 2.29, the raw key rate Alice and Bob can establish depends on the information they share and thereby $\rho_{A,B}$, as $I_{A,B}$ and $\rho_{A,B}$ are related in a monotonically increasing manner. Therefore, with increased turbulence degrees, the raw key rate decreases. This is consistent with existing literature (Wang et al., 2018a). This scientific paper shows that the key rate drastically decreases with decreased transmittance due to beam wandering, broadening, deformation and scintillation. As stated in section 2.5.2, these type of transmittance losses are due to atmospheric turbulence. (Villaseñor et al., 2020; Dequal et al., 2021) imply similarly that the turbulence effect decrease the key rates achievable in free space CV-QKD.

4.2 Bob and Eve with the same turbulence at different parts of the beam

As described in section 3.3, the experiment was then undertaken with Bob and Eve experiencing the same turbulence degrees, but with Eve displaced from the centre of the beam. Here two different displacements where chosen for Eve. The correlation between Alice and Bob is $\rho_{A,B}$ and is calculated using 3.1, where Alice is x and Bob is y. $\rho_{A,E}$ refers to the correlation between Alice and Eve, from equation 3.1 Alice is x and Eve is y. In this part of the experiment there is a distinction between Bob and Eve as there are no longer taking measurements at the same point. Table 3.1 shows the turbulence degrees chosen for this part of the experiment, where

the wavefront distortions used at the DM can be seen in the Appendix A. Here the turbulence degree increases from t_a to t_c. This is due to the fact that smaller order Zernike polynomials have a greater contribution to an increased turbulence effect as stated in section 2.5.1 and seen in equation 2.41.

The real world analogy to this experiment, Bob and Eve are both at separate ground stations. Since Alice and Bob are attempting to establish a secret key, the channel between them will be aligned in such a way, that Bob is in the centre of the beam. Eve, on the other hand is attempting to eavesdrop on them at a separate ground station and is therefore misaligned with the centre of the Alice and Bob's channel beam. Since Eve is not intercepting the data in-between Alice and Bob, her eavesdropping can go undetected (given she is a sufficient distance from Bob's ground station in order for him not to see Eve's ground station receiver). As seen in section 1, the detection of Eve's presence relies on the disturbance of transmission. To calculate Eve's displacements for a real scenario first the beam divergence must be calculated. Assuming a point source beam divergence θ_{BD} in radians can be calculated as such (Chu et al., 2021):

$$\theta_{BD} = 1.22\frac{\lambda}{D_{tx}}, \tag{4.1}$$

where λ is the operating wavelength and D_{tx} is the transmitter telescope aperture size. The beam divergence can now be used to calculate the beam size at the earth surface. For a Low Earth Orbit (LEO) satellite at an altitude of $500km$, $D_{tx} = 10cm$ and $\lambda = 1550nm$ Eve's displacement translates to approximately $2.6m$ and $5.3m$ with a total beam radius of $9.5m$ at the earth's surface.

The initial results of the experiment must be normalised using the correlation $\rho_{A,B}$ in free space without turbulence in the channel as shown in table 4.1. The normalisation is done by dividing the experimental results by $\rho_{A,B}$ in free space without turbulence in the channel as shown in the second column of table 4.1. Using these corrections the the correlation $\rho_{A,E}$ for Eve displaced by 27.8% of beam radius in comparison to $\rho_{A,B}$, as function of turbulence degree with turbulence degree increasing from $t_a - tc$, can be seen in figure 4.2. Figure 4.3 shows how $\rho_{A,E}$, for Eve displaced by 55.6% of the beam radius, behaves compared to $\rho_{A,B}$ as a function of turbulence degree with the turbulence degree increasing from $t_a - t_c$. Figure 4.4 shows the normalised correlations $\rho_{A,B}$ and $\rho_{A,E}$ (with Eve displaced from the centre by displaced 27.8% and 55.6% of the beam radius) for a given turbulence degree as a function of displacement by radius percentage.

Figure 4.2 shows a correlation reduction with increased turbulence degree for both $\rho_{A,B}$ and $\rho_{A,E}$. The figure also shows reduced correlation of $\rho_{A,E}$ compared with $\rho_{A,B}$ at the same turbulence degrees. Here $\rho_{A,B}$ is the correlation between Alice and Bob with Bob at the centre of the beam and $\rho_{A,E}$ is the correlation between Alice and Eve with eve displaced from the beam centre by 27.8% of the beam radius.

Figure 4.3 shows a correlation reduction with increased turbulence degree for both $\rho_{A,B}$ and $\rho_{A,E}$. The figure also shows reduced correlation of $\rho_{A,E}$ compared with $\rho_{A,B}$ at the same turbulence degrees. Here $\rho_{A,B}$ is the correlation between Alice and Bob with Bob at the centre of the beam and $\rho_{A,E}$ is the correlation between Alice and Eve with eve displaced from the beam centre by 55.6% of the beam radius.

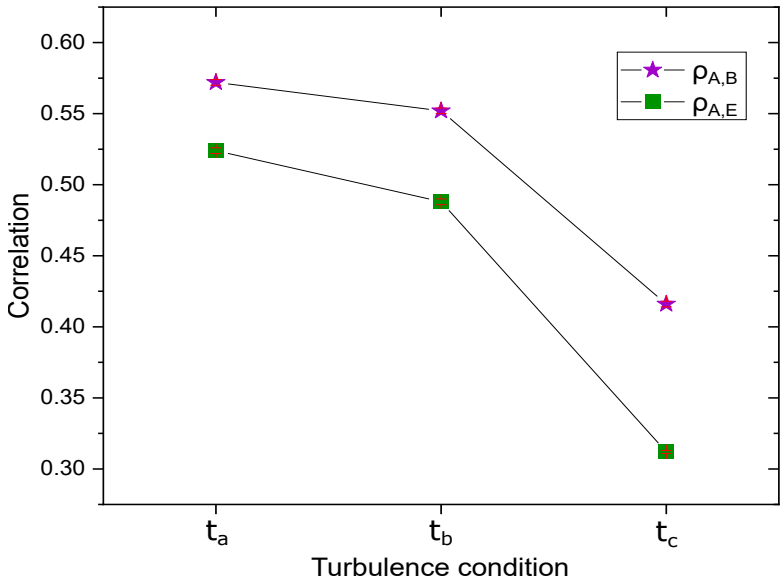

FIGURE 4.2: Normalised results $\rho_{A,E}$ with displacement 27.8% of the beam radius. Where the strength of turbulence increases from t_a to t_c and the error is shown in red. Here $\rho_{A,E}$ refers to the correlation between Alice and Eve, from equation 3.1 Alice is x and Eve is y. The x-axis is not necessarily linear.

Figure 4.4 shows a correlation reduction with increased displacement from the beam centre. The correlation is further reduced when the turbulence degree is increased. Here, at 0% displacement from the beam radius, is the correlation between Alice and Bob. For correlations with displacements, are the correlations for Alice and Eve for Eve's respective displacements form the centre of the beam.

From the results of Bob and Eve comparing the same turbulence degrees with Eve displaced from the centre of the beam, with Eve displaced by 27.8% of the beam radius shown in figure 4.2 and Eve displaced by 55.6% of the beam radius shown in figure 4.3, shows that the correlation $\rho_{A,E}$ is reduced with increasing turbulence degree, which is consistent with the results measured at the centre of the beam with increasing turbulence degrees discussed in the section above, 4.1.

The correlation is reduced as the receiver is displaced from the centre. Here with an increased displacement the correlation is reduced as seen in figure 4.4. Comparing the correlation difference of $\rho_{A,B}$ at the centre of the beam with $\rho_{A,E}$ at the different displacements, as shown in table 4.2 for Eve displaced by 27.8% of the beam radius and table 4.3 for Eve displaced by 55.6% of the beam radius, the correlation difference $\rho_{A,B}$ and displaced $\rho_{A,E}$ increases with increasing turbulence degrees. This increase is larger when Eve has a greater displacement from the centre with the beam. The reduction of correlation $\rho_{A,E}$ with increasing displacement is consistent with results in (Trinh et al., 2019). This scientific paper shows that, with increased distance between Bob and Eve on the receiver plane, Eve's probability to measure errors increases. This indicates that with larger displacement from Bob, the correlation between Alice and Eve decreases. This is consistent with the results in section 4.2.

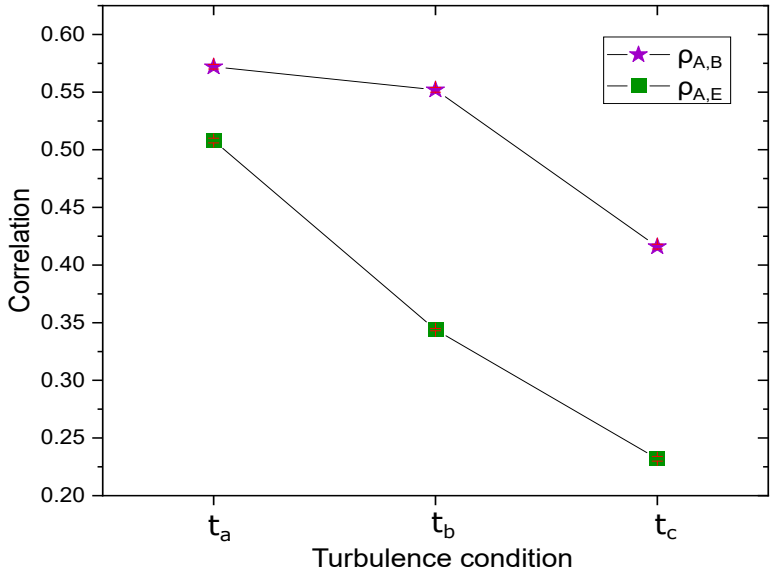

FIGURE 4.3: Normalised results $\rho_{A,E}$ with displacement 55.6% of the beam radius. Where the strength of turbulence increases from t_a to t_c and the error is shown in red. Here $\rho_{A,E}$ refers to the correlation between Alice and Eve, from equation 3.1 Alice is x and Eve is y. The x-axis is not necessarily linear.

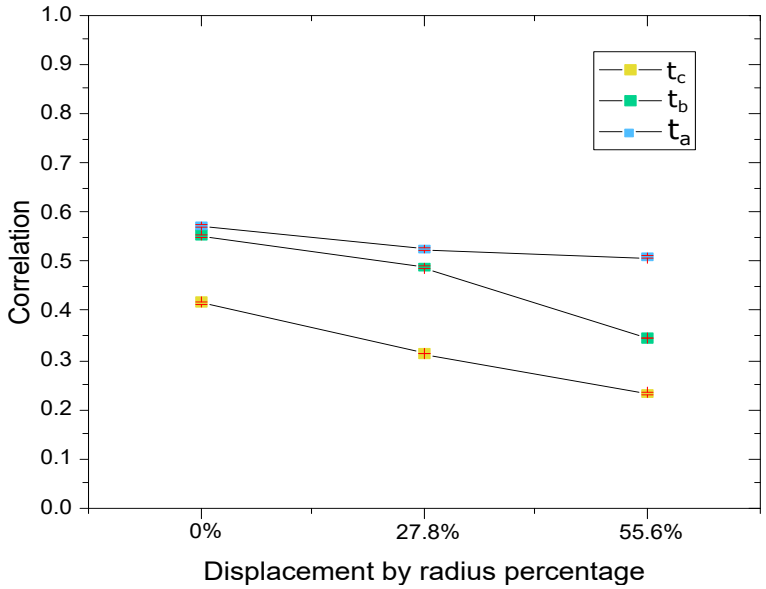

FIGURE 4.4: Normalised correlation results from turbulence degrees $t_a - t_c$ as a function of displacement by radius percentage, where at 0% displacement is the correlation between Alice and Bob. The displacements for 27.8% and 55.6% of the beam radius are the correlations of Alice and Eve where Eve is displaced form the centre of the beam. Here the correlation calculated using 3.1, where Alice is x and Bob is y. For the correlation between Alice and Eve, Alice is x and Eve is y. The error bars are shown in red.

Turbulence degree	$\rho_{A,B} - \rho_{A,E}$, Eve displaced 27.8% of beam radius
t_a	0.048 $\pm$0.002
t_b	0.064 $\pm$0.002
t_c	0.104 $\pm$0.002

TABLE 4.2: Normalised correlation differences $\rho_{A,B}$ and $\rho_{A,E}$ displace by 27.8% of the beam radius for each turbulence degree used.

Turbulence degree	$\rho_{A,B} - \rho_{A,E}$, Eve displaced by 55.6% of the beam radius
t_a	0.064 $\pm$0.002
t_b	0.208 $\pm$0.002
t_c	0.184 $\pm$0.001

TABLE 4.3: Normalised correlation differences $\rho_{A,B}$ and $\rho_{A,E}$ displace by 55.6% of the beam radius for each turbulence degree used.

From equation 2.29, the raw key rate that can be established between Alice and Bob depends on the information shared by Bob and Eve after reverse reconciliation, $\chi_{B,E}$, and the information shared between Alice and Bob, $I_{A,B}$. Reverse reconciliation is used to reduce the information Eve has on the key. Since $\chi_{B,E}$ is proportional to the information shared by Alice and Eve, and this is parameter in turn is related in a monotonically increasing manner to $\rho_{A,E}$, $\chi_{B,E}$ is reduced if the correlation between Alice and Eve is reduced. Now the results indicate that the raw key rate could be increased, if $I_{A,B}$ can be increased.

The results presented in this chapter show that with increasing turbulence degree, the correlation measured between Alice and Bob as well as Alice and Eve decreases. They also show that when Eve is displaced from the centre of the beam her correlation with Alice decreases compared to the correlation between Alice and Bob, where Bob is at the centre of the beam. As stated at the beginning of this chapter, when Alice and Bob have a larger correlation compared to Alice and Eve, Eve has less information, and the channel is therefore more secure. The overall results from this chapter, the potential for future work, will all be presented in the following chapter, chapter 5.

Chapter 5

Conclusion

In this experiment the effect of atmospheric turbulence for satellite to ground CV-QKD was analysed. First as a reference how increasing turbulence degrees affects the correlation between Alice and Bob, then the effect of varying atmospheric turbulence degrees on the channel coherence of Alice and Bob with that of Alice and Eve, where Eve is assumed to be passive at the same ground level as Bob, with Bob at the beam centre and Eve taking measurements in the surrounding areas of the beam. This was done using two different displacements for Eve. Satellite CV-QKD was emulated and the correlation between Alice and Bob were compared with correlation between Alice and Eve. The emulation was done in the lab with the atmospheric turbulence emulated using Zernike polynomials and a deformable mirror.

5.1 Importance of Results

From the sections 4.1 and 4.2, the correlation $\rho_{A,E}$ with passive Eve at a ground station with increasing turbulence degree is reduced compared to $\rho_{A,B}$ at the centre of the beam. This means Eve has less information on the raw key established by Alice and Bob. The raw key between Alice and Bob is generated using the data they share, this means that the more correlated Alice and Bob are, the larger the raw key is that they can establish. The security of this raw key depends on the information Eve has, therefore decreasing correlation between Alice and Eve increases the security of the exchange between Alice and Bob. Now with Eve's decreased knowledge, from equation 1.1 the signal strength can be increased as mentioned in section 1. Therefore, due to atmospheric turbulence the satellite distance and the key rate can be improved since the turbulence impact to the correlation between Alice and Eve is greater than for Alice and Bob, for the case of a passive off-axis Eve. Larger distances are great milestones for CV-QKD, as currently these are inhibiting factors of its real world implementation. For this reason satellite QKD was first suggested to replace fibre QKD, as fibre has a distance limit of around a few hundred kilometers. With increased key rates, QKD is performed more rapidly. This is currently also a limiting factor of satellite CV-QKD. The results show that under passive eavesdropping conditions, it may be possible to increase the key rate and distance of CV-QKD transmission. The results shown in figure 4.4 also indicated, due to atmospheric turbulence, the correlation differs at different sections of the beam. Therefore, at different sections of the beam different quadratures are measured.

This experiment also shows the relative security of a passive eavesdropper at a ground station. As mentioned in section 4.2, Eve on a ground station is not detectable by Alice and Bob since they rely on transmission disturbances to detect Eve. Therefore, with sufficient distance from Bob's ground station Eve can eavesdrop undetected. The results in figure 4.4 imply that with larger distance from Bob, Alice

and Eve's correlation will decrease, and consequently their shared information will also decrease. So, due to the effect of atmospheric turbulence, Eve will have less information about the raw key the further her ground station is away from Bob's. For Eve to improve her information about the raw key she will have to place her ground station closer to Bob's, increasing her chance to be detected by him.

As, in this experiment the atmospheric turbulence is emulated using the change in refractive indices (using a DM), these are the same affects all free-space CV-QKD schemes experience due to atmospheric turbulence. Therefore, results of this experiment should also be applicable for other free-space CV-QKD systems, such as up-links and terrestrial free-space CV-QKD schemes. Although, up-links are rarely used, as mentioned in section 2.4.2 conventionally down-links are used instead of up-links, there are up-link systems currently in use. One of these up-link schemes is the Canadian NanoQEY up-link (Bedington, Arrazola, and Ling, 2017), although it also plans to explore down-links as well. Experiments investigating terrestrial free-space CV-QKD are also not uncommon. For example such schemes are useful for mid-range free-space CV-QKD in dense Urban areas (Brougham and Oi, 2021).

In this experiment the objective was to test how atmospheric turbulence effects the comparative correlation for satellite to ground CV-QKD of Alice and Bob, and Alice and Eve, where Eve is considered passive and displaced from the centre of the beam at a ground station with Bob at the centre of the beam at a ground station. This was achieved by first testing the effect of atmospheric turbulence on the correlation of CV-QKD and then comparing the correlations $\rho_{A,B}$ and $\rho_{A,E}$ with Eve at two different locations of the beam. This was done by emulating satellite CV-QKD in the laboratory, with a DM used to emulate atmospheric turbulence between Alice, Bob and Eve.

The results show that with increasing turbulence degrees, the correlation between Alice and Bob, and Alice and Eve decrease as expected. The correlation between Alice and Bob, with Bob at the centre of the beam, is comparatively greater than the correlation between Alice and Eve regardless of the turbulence strength. The correlation between Alice and Eve decreases the further Eve is displaced from the centre of the beam. This in consistent with the expected results.

As this was a laboratory experiment, there are limitations to it compared to a real world scenario. In this experiment the turbulence was only emulated using a DM, with an emulation the atmospheric turbulence is only approximated. In addition, in a real world scenario, it is possible for Bob's ground station to examine at which distances Eve can go undetected by him. Here this was only estimated using a calculation (see section 4.2). The experiment could also be improved by adding the post processing back to the CV-QKD protocol. With the post processing the key rates can be calculated rather than estimating their increase and decease, as done in section 4. The amount of information Eve has about the key can also be calculated. With post processing reverse and direct reconciliation can be compared for this scenario. From the conclusion of this experiment, reverse reconciliation should out perform direct reconciliation. As Eve's measurements will differ from Bob's due to the atmospheric turbulence effect. The measurements will differ more, the further Eve's ground station is from Bob's. This means reverse reconciliation will out perform direct reconciliation increasingly, when Eve's ground station is placed at increasing

distances from Bob's ground station.

The results discussed above can be used in future work. Now in future CV-QKD projects, for line of sight satellite to ground CV-QKD under passive eavesdropping (as well as all other free-space CV-QKD schemes), the signal strength can be increased to improve the correlation between Alice and Bob. This is possible, as the atmospheric turbulence will have a larger impact on reducing the correlation between Alice and a displaced Eve than reducing the correlation between Alice and Bob. With an increased signal strength, the raw key rate over the turbulent channel can be increased and this will greatly improve the free space communication.

Appendix A

Wavefront distortion modeled by the Deformable Mirror

Here are the images depicting how differing Zernike polynomials affect the DM. These images snapshots of the DM's software. As stated in section 3.3.3 the DM used was from Thorlabs (DMP40/M-P01) with the software used from the provider. Using this software, the Zernike polynomials can be manipulated and the wavefront distortions are generated. These distortion mimic the wavefront distortions generated by atmospheric turbulence. The wavefront depicted in the images below are shown in table 3.1. How Zernike polynomials model turbulence is shown in section 2.5.1, where equation 2.41 shows how Zernike polynomials model wavefront distortion. Here smaller order Zernike polynomials have a larger contribution to the wavefront distortion and therefore a smaller order Zernike polynomials contribute to a increased turbulence affect.

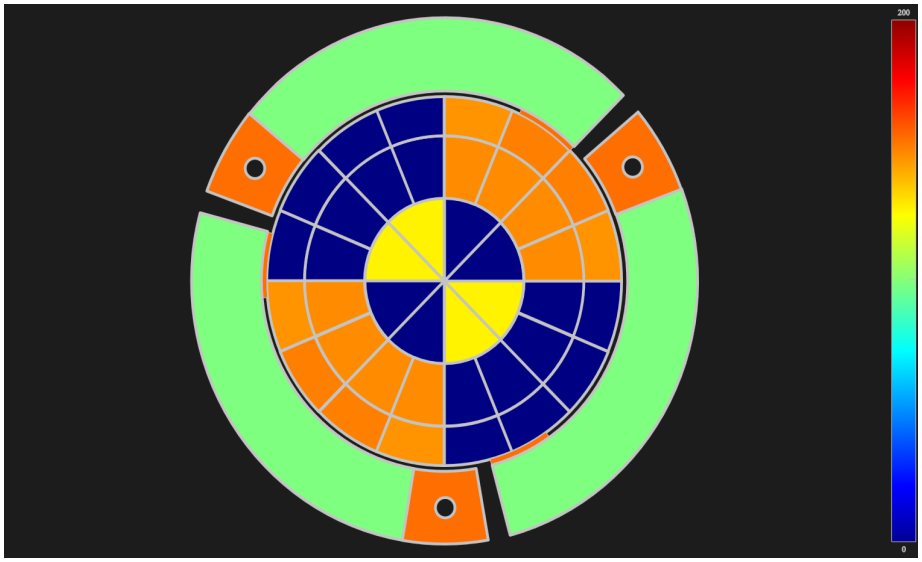

FIGURE A.1: Wavefront distortion on the DM when $Z_4 = 1$ $Z_5 = -0.5$ with the DM set to low turbulence from the internal software settings. Here the scale indicates the amount of voltage that goes through the individual sections of the DM, where increased voltage indicates a larger change in the refractive index. The legend on the right shows the voltage through the DM segments and ranges from $0mV$ to $200mV$.

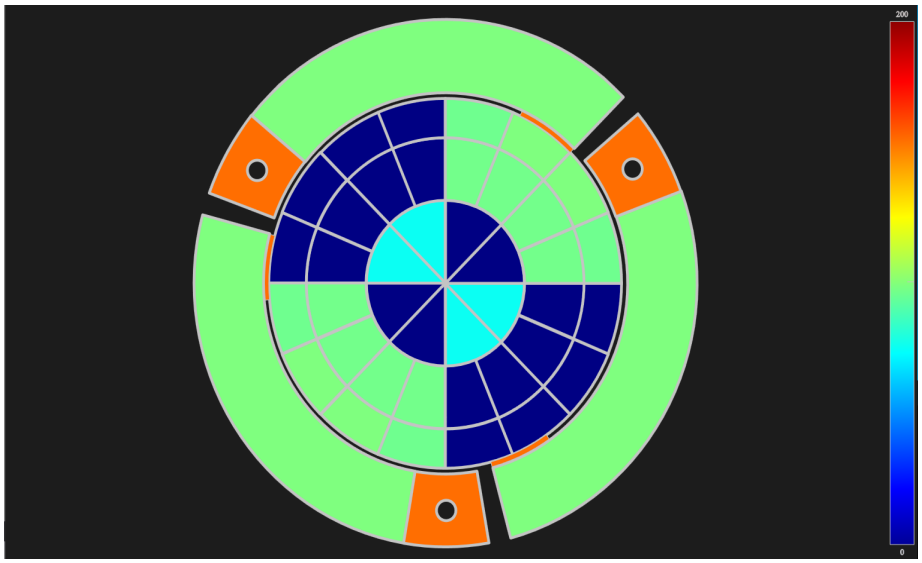

FIGURE A.2: Wavefront distortion on the DM when $Z_4 = 1$ with the DM set to low turbulence from the internal software settings. Here the scale indicates the amount of voltage that goes through the individual sections of the DM, where increased voltage indicates a larger change in the refractive index. The legend on the right shows the voltage through the DM segments and ranges from $0mV$ to $200mV$.

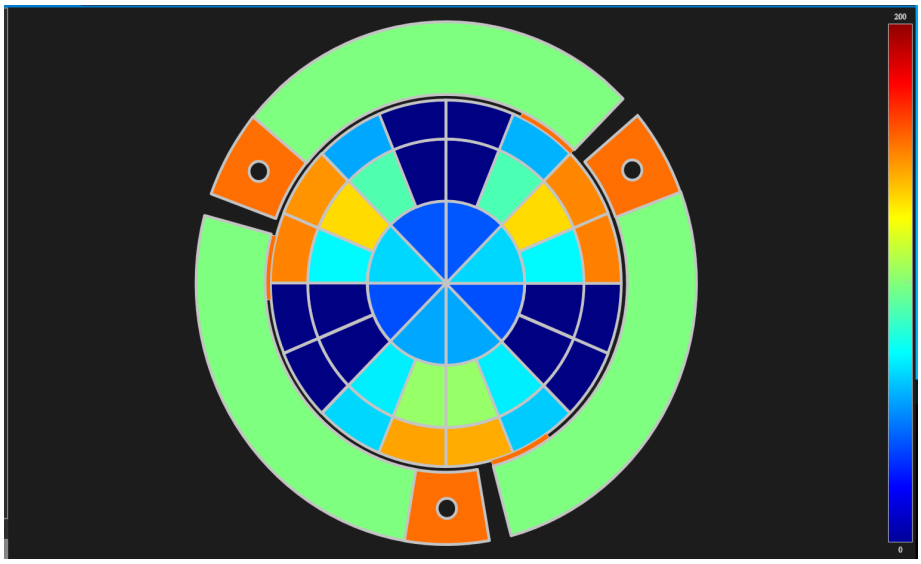

FIGURE A.3: Wavefront distortion on the DM when $Z_5 = -0.5$ $Z_7 = 1$ with the DM set to low turbulence from the internal software settings. Here the scale indicates the amount of voltage that goes through the individual sections of the DM, where increased voltage indicates a larger change in the refractive index. The legend on the right shows the voltage through the DM segments and ranges from $0mV$ to $200mV$.

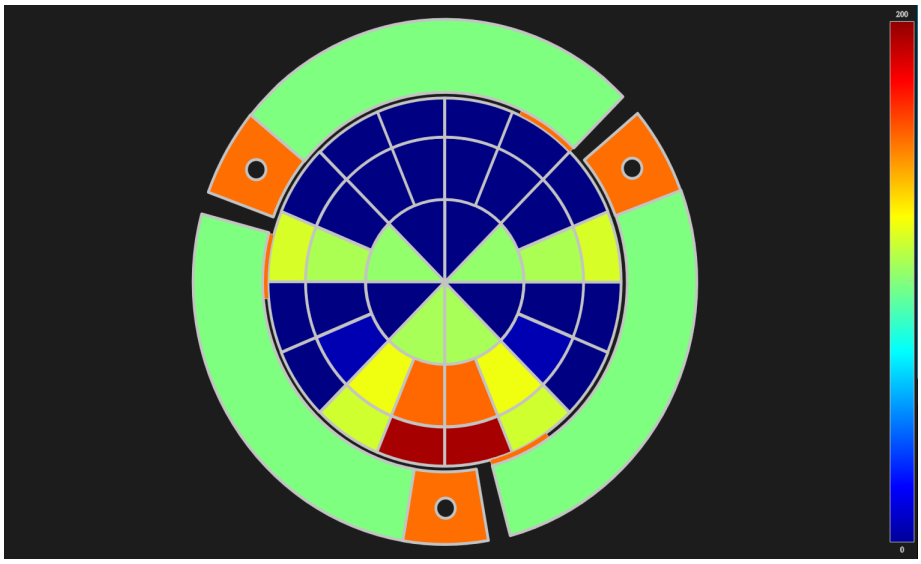

FIGURE A.4: Wavefront distortion on the DM when $Z_7 = -1$ $Z_8 = 1$ with the DM set to low turbulence from the internal software settings. Here the scale indicates the amount of voltage that goes through the individual sections of the DM, where increased voltage indicates a larger change in the refractive index. The legend on the right shows the voltage through the DM segments and ranges from $0mV$ to $200mV$.

List of Abbreviations

QKD	**Q**uantum **K**ey **D**istribution
DV	**D**iscrete **V**ariable
CV	**C**ontinuous **V**ariable
LO	**L**ocal **O**scillator
PD	**P**hoto **D**iode
SNR	**S**ignal to **N**oise **R**atio
LLO	**L**ocal **L**ocal **O**scillator
TLO	**T**ransmitted **L**ocal **O**scillator
FG	**F**unction **G**enerator
DAQ	**D**ata **A**c**Q**uisition
DM	**D**eformable **M**irror
AM	**A**mplitude **M**odulator
PM	**P**hase **M**odulator
PBS	**P**olarising **B**eam**S**plitter
FM	**F**araday **M**irror
LEO	**L**ow **E**arth **O**rbit

Bibliography

Adesso, Gerardo, Sammy Ragy, and Antony R Lee (2014). "Continuous variable quantum information: Gaussian states and beyond". In: *Open Systems & Information Dynamics* 21.01n02, p. 1440001.

Arteaga-Díaz, Pablo, Alejandro Ocampos-Guillén, and Veronica Fernandez (2019). "Enabling QKD under strong turbulence for wireless networks with tilt wavefront correction". In: *2019 21st International Conference on Transparent Optical Networks (ICTON)*. IEEE, pp. 1–4.

Bedington, Robert, Juan Miguel Arrazola, and Alexander Ling (2017). "Progress in satellite quantum key distribution". In: *npj Quantum Information* 3.1, pp. 1–13.

Bennett, Charles H and Gilles Brassard (2020). "Quantum cryptography: Public key distribution and coin tossing". In: *arXiv preprint arXiv:2003.06557*.

Bonato, Cristian et al. (2009). "Feasibility of satellite quantum key distribution". In: *New Journal of Physics* 11.4, p. 045017.

Brougham, T and DKL Oi (2021). "Medium-range terrestrial free-space QKD performance modelling and analysis". In: *Quantum Technology: Driving Commercialisation of an Enabling Science II*. Vol. 11881. SPIE, pp. 14–23.

Chen, Peter Y, Michael Smithson, and Paula M Popovich (2002). *Correlation: Parametric and nonparametric measures*. 139. Sage.

Chu, Yi et al. (2021). "Feasibility of quantum key distribution from high altitude platforms". In: *Quantum Science and Technology* 6.3, p. 035009.

Cooper, Merlin et al. (2013). "Experimental generation of multi-photon Fock states". In: *Optics express* 21.5, pp. 5309–5317.

Dadson, Simon James (2017). *Statistical Analysis of Geographical Data: An Introduction*. John Wiley & Sons.

De Oliveira, FAM et al. (1990). "Properties of displaced number states". In: *Physical Review A* 41.5, p. 2645.

Dequal, Daniele et al. (2021). "Feasibility of satellite-to-ground continuous-variable quantum key distribution". In: *npj Quantum Information* 7.1, pp. 1–10.

Diamanti, Eleni and Anthony Leverrier (2015). "Distributing secret keys with quantum continuous variables: principle, security and implementations". In: *Entropy* 17.9, pp. 6072–6092.

Diamanti, Eleni et al. (2016). "Practical challenges in quantum key distribution". In: *npj Quantum Information* 2.1, pp. 1–12.

Dieks, DGBJ (1982). "Communication by EPR devices". In: *Physics Letters A* 92.6, pp. 271–272.

Ding, Kemi et al. (2020). "Remote state estimation in the presence of an active eavesdropper". In: *IEEE Transactions on Automatic Control* 66.1, pp. 229–244.

Fante, Ronald L (1975). "Electromagnetic beam propagation in turbulent media". In: *Proceedings of the IEEE* 63.12, pp. 1669–1692.

Ficek, Zbigniew and Mohamed Ridza Wahiddin (2014). *Quantum optics for beginners*. CRC Press.

Garrison, John and Raymond Chiao (2008). *Quantum optics*. OUP Oxford.

Gerrits, Thomas, S Glancy, and Sae Woo Nam (2011). "A balanced homodyne detector and local oscillator shaping for measuring optical Schrödinger cat states". In: *Advanced Photon Counting Techniques V*. Vol. 8033. SPIE, pp. 262–268.

Gerry, Christopher, Peter Knight, and Peter L Knight (2005). *Introductory quantum optics*. Cambridge university press.

Grosshans, Frédéric and Philippe Grangier (2002a). "Continuous variable quantum cryptography using coherent states". In: *Physical review letters* 88.5, p. 057902.

— (2002b). "Reverse reconciliation protocols for quantum cryptography with continuous variables". In: *arXiv preprint quant-ph/0204127*.

Grosshans, Frédéric et al. (2003). "Quantum key distribution using gaussian-modulated coherent states". In: *Nature* 421.6920, pp. 238–241.

Hirano, Takuya et al. (2017). "Implementation of continuous-variable quantum key distribution with discrete modulation". In: *Quantum Science and Technology* 2.2, p. 024010.

Hosseinidehaj, Nedasadat et al. (2018). "Satellite-based continuous-variable quantum communications: State-of-the-art and a predictive outlook". In: *IEEE Communications Surveys & Tutorials* 21.1, pp. 881–919.

Huang, Duan et al. (2016). "Long-distance continuous-variable quantum key distribution by controlling excess noise". In: *Scientific reports* 6.1, pp. 1–9.

Jouguet, Paul, Sébastien Kunz-Jacques, and Anthony Leverrier (2011). "Long-distance continuous-variable quantum key distribution with a Gaussian modulation". In: *Physical Review A* 84.6, p. 062317.

Jouguet, Paul et al. (2012). "Analysis of imperfections in practical continuous-variable quantum key distribution". In: *Physical Review A* 86.3, p. 032309.

Jouguet, Paul et al. (2013). "Experimental demonstration of long-distance continuous-variable quantum key distribution". In: *Nature photonics* 7.5, pp. 378–381.

Kish, Sebastian et al. (2020). "Use of a Local Local Oscillator for the Satellite-to-Earth Channel". In: *arXiv preprint arXiv:2010.09399*.

Kish, SP et al. (2021). "Use of a local local oscillator for the satellite-to-earth channel". In: *ICC 2021-IEEE International Conference on Communications*. IEEE, pp. 1–6.

Král, P (1990). "Displaced and squeezed Fock states". In: *Journal of Modern Optics* 37.5, pp. 889–917.

Kumar, Rupesh, Hao Qin, and Romain Alléaume (2015). "Coexistence of continuous variable QKD with intense DWDM classical channels". In: *New Journal of Physics* 17.4, p. 043027.

Leverrier, Anthony et al. (2008). "Multidimensional reconciliation for a continuous-variable quantum key distribution". In: *Physical Review A* 77.4, p. 042325.

Liang, Yingbin, H Vincent Poor, Shlomo Shamai, et al. (2009). "Information theoretic security". In: *Foundations and Trends® in Communications and Information Theory* 5.4–5, pp. 355–580.

Liao, Sheng-Kai et al. (2017). "Satellite-to-ground quantum key distribution". In: *Nature* 549.7670, pp. 43–47.

Lodewyck, Jérôme et al. (2007). "Quantum key distribution over 25 km with an all-fiber continuous-variable system". In: *Physical Review A* 76.4, p. 042305.

Noll, Robert J (1976). "Zernike polynomials and atmospheric turbulence". In: *JOsA* 66.3, pp. 207–211.

Pirandola, Stefano (2021). "Limits and security of free-space quantum communications". In: *Physical Review Research* 3.1, p. 013279.

Pirandola, Stefano et al. (2020). "Advances in quantum cryptography". In: *Advances in Optics and Photonics* 12.4, pp. 1012–1236.

Popoola, Wasiu et al. (2009). "Atmospheric channel effects on terrestrial free space optical communication links". In: *3rd international conference on computers and artificial intelligence (ECAI 2009)*. Citeseer, pp. 17–23.

Qi, Bing et al. (2015). "Generating the local oscillator "locally" in continuous-variable quantum key distribution based on coherent detection". In: *Physical Review X* 5.4, p. 041009.

Qin, Hao, AQ Huang, and Vadim Makarov (2017). *Short pulse attack on continuous-variable quantum key distribution system*.

Qu, Zhen and Ivan B Djordjevic (2017). "Approaching Gb/s secret key rates in a free-space optical CV-QKD system affected by atmospheric turbulence". In: *2017 European Conference on Optical Communication (ECOC)*. IEEE, pp. 1–3.

Ralph, Tim and Ping Koy Lam (2013). "Don't cry over broken entanglement". In: *Physics* 6, p. 74.

Ralph, Timothy C (1999). "Continuous variable quantum cryptography". In: *Physical Review A* 61.1, p. 010303.

— (2000). "Security of continuous-variable quantum cryptography". In: *Physical review A* 62.6, p. 062306.

Reid, Margaret D (2000). "Quantum cryptography with a predetermined key, using continuous-variable Einstein-Podolsky-Rosen correlations". In: *Physical Review A* 62.6, p. 062308.

Renner, Renato, Nicolas Gisin, and Barbara Kraus (2005). "Information-theoretic security proof for quantum-key-distribution protocols". In: *Physical Review A* 72.1, p. 012332.

Schatz, PN and AJ McCaffery (1969). "The faraday effect". In: *Quarterly Reviews, Chemical Society* 23.4, pp. 552–584.

Shao, Yun et al. (2021). "Phase noise model for continuous-variable quantum key distribution using a local local oscillator". In: *Physical Review A* 104.3, p. 032608.

Shen, Yong et al. (2014). "A fiber-based quasi-continuous-wave quantum key distribution system". In: *Scientific reports* 4.1, pp. 1–5.

Shor, Peter W (1994). "Algorithms for quantum computation: discrete logarithms and factoring". In: *Proceedings 35th annual symposium on foundations of computer science*. Ieee, pp. 124–134.

Strickland, Donna and G Morou (1985). "Chirped pulse amplification". In: *Opt. Comm* 56, p. 219.

Tomaello, Andrea et al. (2011). "Link budget and background noise for satellite quantum key distribution". In: *Advances in Space Research* 47.5, pp. 802–810.

Trinh, Phuc V et al. (2019). "Effects of atmospheric turbulence and misalignment-induced fading on the secrecy performance of IM/DD free-space CV-QKD systems using a Gaussian beam". In: *International Conference on Space Optics—ICSO 2018*. Vol. 11180. International Society for Optics and Photonics, 111801Y.

Vagniluca, Ilaria et al. (2020). "Efficient time-bin encoding for practical high-dimensional quantum key distribution". In: *Physical Review Applied* 14.1, p. 014051.

Van Assche, Gilles, Jean Cardinal, and Nicolas J Cerf (2004). "Reconciliation of a quantum-distributed Gaussian key". In: *IEEE Transactions on Information Theory* 50.2, pp. 394–400.

Villaseñor, Eduardo et al. (2020). "Atmospheric effects on satellite-to-ground quantum key distribution using coherent states". In: *GLOBECOM 2020-2020 IEEE Global Communications Conference*. IEEE, pp. 1–6.

Voss, Paul (2009). "OPTICAL HOMODYNE DETECTION AND APPLICATIONS IN QUANTUM CRYPTOGRAPHY". PhD thesis. Citeseer.

Walls, Daniel F and Gerard J Milburn (2007). *Quantum optics*. Springer Science & Business Media.

Wang, H et al. (2008). "Measurement of the decay of Fock states in a superconducting quantum circuit". In: *Physical Review Letters* 101.24, p. 240401.

Wang, Ping et al. (2021). "Robust frame synchronization for free-space continuous-variable quantum key distribution". In: *Optics Express* 29.16, pp. 25048–25063.

Wang, Shiyu et al. (2018a). "Atmospheric effects on continuous-variable quantum key distribution". In: *New Journal of Physics* 20.8, p. 083037.

Wang, Tao et al. (2018b). "High key rate continuous-variable quantum key distribution with a real local oscillator". In: *Optics express* 26.3, pp. 2794–2806.

Wang, Xiang-Bin et al. (2007). "Quantum information with Gaussian states". In: *Physics reports* 448.1-4, pp. 1–111.

Wang, Xiangyu et al. (2017). "Efficient rate-adaptive reconciliation for continuous-variable quantum key distribution". In: *arXiv preprint arXiv:1703.04916*.

Weedbrook, Christian et al. (2012). "Gaussian quantum information". In: *Reviews of Modern Physics* 84.2, p. 621.

Wootters, William K and Wojciech H Zurek (1982). "A single quantum cannot be cloned". In: *Nature* 299.5886, pp. 802–803.

Xu-Yang, Wang et al. (2013). "Four-state modulation continuous variable quantum key distribution over a 30-km fiber and analysis of excess noise". In: *Chinese Physics Letters* 30.1, p. 010305.

Zhan, Hanyu, Erandi Wijerathna, and David Voelz (2020). "Is the formulation of the Fried parameter accurate in the strong turbulent scattering regime?" In: *OSA Continuum* 3.9, pp. 2653–2659.

Zhang, Wei-Min, Robert Gilmore, et al. (1990). "Coherent states: theory and some applications". In: *Reviews of Modern Physics* 62.4, p. 867.

Zhou, Guangping and Anup Shrestha (2013). "Efficient intrusion detection scheme based on SVM". In: *Journal of networks* 8.9, pp. 2128–2134.