Protocols and Resources for New Generation Continuous Variable Quantum Key Distribution

Oliver Thearle

A thesis submitted for the degree of
Doctorate of Philosophy in Engineering at
The Australian National University

August 2017

Declaration

This thesis is an account of research undertaken between February 2013 and August 2017 at The Research School of Engineering and The Department of Quantum Science, Research School of Physics and Engineering, The Australian National University, Canberra, Australia.

Except where acknowledged in the customary manner, the material presented in this thesis is, to the best of my knowledge, original and has not been submitted in whole or part for a degree in any university.

Oliver Thearle
August, 2017

To my parents for supporting me through my bad decisions.

Acknowledgments

Firstly I would like acknowledge and thank my supervisory panel, Matt James, Jiri Janousek, Ping Koy Lam and Elanor Huntington and honorary member Syed Assad. You have all been very supportive of my research throughout my candidature. Your collective experience has provided me with valuable insight into research and quantum optics. Each one of you has greatly contributed towards the completion of this thesis. Thank you all so much for giving me the opportunity to complete a PhD.

Secondly I would like to thank the ANU quantum optics group and the whole of the department of quantum science for providing me a friendly environment to complete my thesis. There are far to many of you to list but through the many varied social activities the community of DQS has greatly contributed to enriching my time at ANU. My 1064 office and lab buddies, Jing-Yan Haw, Zhao Jie, Syed Assad, Mark Bradshaw, Thibault Michel, Hao Jeng and past members Seiji Armstrong, Helen Chrzanowski, Sara Hosseini, Jiao Geng, Alex Brieussel, thanks for putting up with me for so long even if I did tell some of you to be quiet for science from time to time. Thank you to Seiji, Jiri, Sara, Melanie Schünemann (Mraz) and many others for persevering with me through the Bell test experiment. After many years it is finally published. Thank you to Georgia Mansell for the random food, tea and for always making sure I went to the CGP Christmas party. Most importantly thank you to Amanda Haines (White) and Lynne Christians for the many Tim Tams and helping me navigate through the ANU bureaucracy.

My thanks to the climbing gang that I spent many weekends with talking and sometimes climbing with. Geoff Campbell, Chris 'Bearded Chris' Hunter Lean, Aaron Trantor, Giovanni Guccioni, Pierre Vernaz-Gris, Jess Eastman and the many others that I've climbed with, thanks for providing me with a fear of falling to distract me from my thesis over the years.

I would also like to thank my friends Joe, Carlie, Richard, Rachel, Peter, Vicki, Jon, Mel, Shaven Chris, Geoff, Ellen, Burgo and Emma. We've had many memorable moments together while I've been a student watching you all progress through life. I'm hoping that now I've finished I can catch up to you all.

Lastly thank you to my immediate family for always being around to support and feed me. Especially to my mum who proof read my thesis in an amazingly short time.

As required by the "Commonwealth Scholarships Guidelines (Research) 2017" I acknowledge the support of the Australian Government through an Australian Government

Research Training Program Scholarship.

This thesis was written and typeset using LaTeX. All of the diagrams were drawn using the latex package Ti*k*z and the plots with the package PGFplots. The inspiration for the drawings came from the free vector image collection of optical components, ComponentLibrary by Alexander Franzen. Each component was recreated using Ti*k*z.

Abstract

Quantum optics has been developing into a promising platform for future generation communications protocols. Much of this promise so far has come from the development of quantum key distribution (QKD). The majority of the development of QKD is done with discrete variables (DV), i.e. qubits with the underlying system of single photons. This is one interpretation of an optical field. Alternatively an optical field can be interpreted as wave with the continuous variable (CV) observables of phase and amplitude. This interpretation comes with the advantage of access to high efficiency detection at room temperature and deterministic sources at the cost of susceptibility to noise in lossy channels.

This thesis presents an investigation of protocols and resources for the next generation of CV QKD protocols with two directions, the development of quantum state resources and the development of QKD protocols.This thesis starts with the details on the on going development of a low loss squeezed state resource using OPA for use in future communication and estimation experiments. So far the OPA has produced 11dB of squeezing with 13dB predicted with reasonable improvements to losses and locking. Being able to perform a Bell test with a CV Bell state is also key for future CV QKD protocols. Originally developed for DV systems the Bell test is a fundamental test of quantum mechanics. Here the first experimental demonstration of an optical CV bell test is presented. The experiment violated a CHSH Bell inequality with $|B| = 2.31$. This violation holds promise for being able to realise new device or source independent CV protocols.

The second half of this thesis proposes a channel parameter estimation protocol based on the method of moments and presents the results of a one side device independent CV QKD demonstration based on the family of Gaussian QKD protocols. The proposed channel parameter estimation protocol through the use of the method of moments is able to use information usually disregarded for estimation of an adversaries information. The result does not allow for an increase in range of a fully optimised protocol but can increase the key rate by an order of magnitude with high loss channels. Using a newly found entroptic uncertainty relation for CV tripartite states a new security proof was applied to the family of Gaussian CV QKD protocols. This resulted in the discovery of six new protocols with the special property of being one side device independent. Using the new security proof three of the protocols were demonstrated with a positive key rate.

Contents

Introduction

Quantum mechanics is a very counter intuitive interpretation of reality with its predictions that go against how we experience the world. This is exemplified by the EPR paradox [1] which predicts a violation of the basic principle of local realism with non-local correlations. With this paradox in mind the famed Bell test [2] was developed and experimentally demonstrated using quantum optics to show that local realism is incorrect [3], albeit with some loopholes that could explain the violation. Recently four Bell test experiments have unequivocally demonstrated a violation of local realism by closing all of the major loopholes [4–7]. The original Bell test was formulated for discrete states and as such all four of these violations were made using single photons states. The study of single photons is part of a sub field of quantum optics known as Discrete Variable (DV) quantum optics. While DV is an interesting area this thesis explores the alternate sub field of Continuous Variable (CV) quantum optics [8] based on the equivalent interpretation of light as a wave. These two interpretations closely link the study of DV and CV quantum optics.

As well as fundamental research quantum optics is also providing a toolbox for a new generation of quantum based communication technologies with a few interesting examples found in Ref. [9–11]. These new technologies will be crucial to realise a future where quantum mechanics will become ubiquitous for solving problems. One set of protocols that has found it way into commercial applications as a solution to the key distribution problem is quantum key distribution (QKD).

The key distribution problem can be described by a game where two parties, Alice and Bob, want to communicate a using a public channel controlled by an eavesdropper, Eve. Alice and Bob can communicate using encryption but the problem is how to distribute the encryption key without Eve intercepting it in a usable form. A common solution to this problem is to use a public key distribution protocol. A famous example of these protocols is the Diffie-Hellman key exchange protocol [12]. Using a combination of private and publicly exchanged information Alice and Bob can distil a shared secret. The finer details of this protocol are outside of the scope of this thesis but the security of the publicly exchanged information relies on the difficult problem of integer factorisation. This is an easy task for small numbers but it becomes exponentially harder for large numbers. In computer science it is believed to be an NP-intermediate problem which is presumed to

be a hard class of problems. While it is currently hard to solve on a classical computer this and other difficult problems might not be so hard on a quantum computer with Shor's algorithm [13].

QKD uses physical principles to ensure security [14, 15]. A QKD protocol will have Alice generate a series of quantum states to send to Bob. Using the properties of quantum mechanics if Eve is listening any interaction she has with the transmitted states will create detectable errors between Alice and Bob. If the error rate is too high Alice and Bob can abort the protocol and try again or try to disassociate their shared secret from Eve's intercepted information. The advantage of QKD is that its security will hold as long as the underlying physical principles do. With classical key distribution protocols Eve can record the transmitted bits. Then at a later date when the particular distribution protocol is broken she can use her records to decrypt any data sent in the past. The advent of general quantum computing has the potential to change how data is communicated and stored. There are efforts to investigate public encryption protocols that are hardened against the potential of quantum computing [16].

This thesis presents an investigation of protocols and resources for the next generation of CV QKD protocols. The protocols investigated through this thesis address two directions in the development of CV QKD, reducing the noise present in a protocol and reducing the number of assumptions required by the security proofs. For some CV QKD protocols the major source of noise comes from the quantum resource states required for the protocol [17]. This thesis addresses the issue of source noise with the results from the development of a low intra-cavity loss OPA squeezed state source that could be used with QKD protocols. Another common source of noise is the overestimation of Eve's information to ensure security in the universal compostability framework. In this thesis the method of moments estimator is demonstrated to reduce the variance of the estimate of the channel noise in high loss channels as compared to the widely used maximum likelihood estimation method thereby placing a tighter bound on Eve's information and increasing the final key rate. To reduce the number of assumptions made in a CV QKD protocol the properties of EPR states can be used. The best possible protocol is one where neither Alice or Bob need to trust quantum and measurement devices and only rely on the outcomes of the measurements. This is possible with a loop-hole free Bell test [18]. This thesis moves towards realising this protocol through the first optical CV Bell test using Gaussian measurements to violate the CHSH inequality. A lesser protocol is one where either only Alice or Bob are required to trust their devices in a one sided device independent protocol (1sDI). This thesis generalises 1sDI to the family of Gaussian CV QKD protocols using a tripartite entropic uncertainty principle allowing the demonstration of three 1sDI CV QKD protocols including the first prepare and measure 1sDI protocol.

Thesis Outline

The structure of this thesis is illustrated in Fig. 1. The content has been split into two parts, Part 1: Quantum State Generation and Part 2: Continuous Variable Quantum Key Distribution. Each part starts with an overview of the material to provide some background and context. Part 1 covers the work that is more general to quantum mechanics and introduces the basic theory used here from the point of view of continuous variable quantum optics in Ch. 1. Building on this theory some of the experimental techninques used in this thesis are presented in Ch. 2. Following this the results from the development of a low intracavity loss OPA are presented in Ch. 3. Ch. 4 will present the results from the first optical CV Bell test. Part 2 covers the work relating specifically to CV QKD. It opens with an introduction to classical and quantum information theory. This chapter applies some of the ideas presented in Ch. 1 and concludes with an introduction to CV QKD. Ch. 6 details the application of the method of moments estimator to CV QKD to estimate the channel noise. The one-sided-device-independent CV QKD protocols with their demonstrations are given in Ch. 7. The thesis is concluded in Ch. 8 with a summary of the key results and a perspective on where the field of CV QKD is headed.

Publications

1. O. Thearle, S. M. Assad, T. Symul, "Estimation of output-channel noise for continuous-variable quantum key distribution," *Physical Review A*, **93**, 042343 (2016).

2. N. Walk, S. Hosseini, J. Geng, O. Thearle, J. Y. Haw, S. Armstrong, S. M. Assad, J. Janousek, T. C. Ralph, T. Symul, H .M. Wiseman, and P. K. Lam, "Experimental demonstration of Gaussian protocols for one-sided device-independent quantum key distribution," *Optica*, **3**, 634-642 (2016).

3. S. M. Assad, O. Thearle, and P. K. Lam "Maximizing device-independent randomness from a Bell experiment by optimizing the measurement settings," *Physcial Review A*, **94**, 012304 (2016).

4. O. Thearle, J. Janousek, S. Armstrong, S. Hosseini, M. Mraz, S. M. Assad, T. Symul, M. R. James, E. Huntington, T. C. Ralph, P. K. Lam, "Violation of Bell's inequality using continuous variable measurements," *Physical Review Letters*, **120**, 040406 (2018).

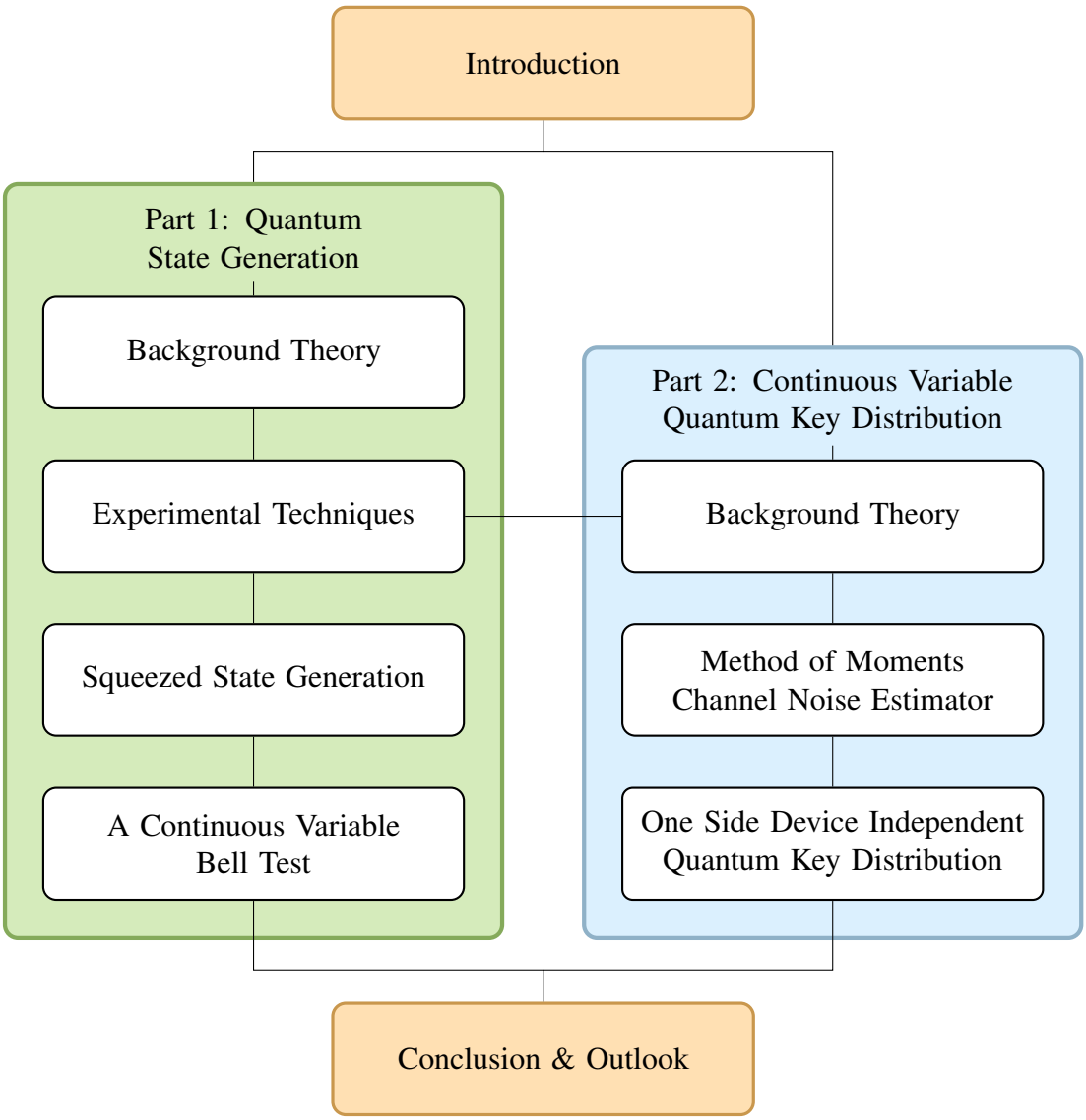


Figure 1: Thesis Outline

Part I

Bell Tests and Quantum State Generation

Overview

Quantum mechanics is not a very intuitive physical description of the world. Some of the more commonly known predictions by quantum mechanics such as Heisenberg's uncertainty principle or entanglement do not align with our experience of the real world. For example it is common to observe local realism in our everyday experience. That is objects around us appear to be in a real predetermined state and are only changed by local effects. However using quantum mechanics, local realism can be shown to not hold true for all systems. First with the thought experiment by Einstein, Podolsky and Rosen [1] where entanglement was first predicted and then more recently by a series of experiments disproving local realism [4–7]. As quantum mechanics is revealing a world unfamiliar to most, it is opening up opportunities to create some interesting technological advances in computing and communications. More often that not these developments in protocols and algorithms are either unrealisable with current abilities or restricted to a laboratory as the states required are difficult to create.

The following chapters will provide an introduction to the mathematics behind quantum mechanics and provide some description on creating and measuring quantum states. Ch. 1 will provide the basic maths and ideas for describing optical quantum states. This chapter will also contain a brief discussion on the experimental techniques used to create and measure quantum states. Ch. 3 will cover some work on creating highly squeezed quantum states which are hoped will be able to be used for quantum protocol demonstrations. The final chapter, Ch. 4 will discuss a continuous variable test of local realism.

The background to this part is mostly given in Ref. [19] and Ref. [13]. Another useful reference for the experimental side is given in Ref. [20]. Much of the work presented has a long history within the research group with much of it document in previous PhD theses. A good example is found in Ref. [21] which contains much of the same background.

Chapter 1

Background Theory

1.1 Quantum mechanics

This section will give a basic description of quantum mechanics for isolated and closed systems in a manner that will be helpful in understanding this thesis. The section is modelled from the postulates of quantum mechanics given in Ref. [13].

1.1.1 State space

In classical mechanics the representation of information is in bits. This unit of information is common and can be found in computing and communication theory. In practical systems the bit is encoded into two level systems such as a coin. A coin flip will put the coin into one of two states, either heads up or tails up. In quantum mechanics the analogue to a bit is a qubit which describes a two level system that is more complex as the system is allowed to be in a superposition between states. A quantum state can be described by a state vector which is a unit vector in a Hilbert space that describes the state space of the physical system of the quantum state. A Hilbert space is complex vector space with an inner product. For a qubit the state space is described by the orthonormal basis $\{|0\rangle, |1\rangle\}$. Here $|i\rangle$ represents a vector in the state space using the ket notation. An arbitrary qubit state in this basis is written as,

$$|\phi\rangle = a|0\rangle + b|1\rangle \tag{1.1}$$

The inner product is then given by $\langle\phi|\phi\rangle = 1$, where $\langle\phi|$ is the vector dual of $|\phi\rangle$. The result of the inner product satisfies the requirement that the state vector be a unit vector on the state space. In general an arbitrary pure state can be represented as a linear combination of the eigenstates.

1.1.2 Evolution

A closed quantum system can evolve through time with the evolution of a state at time $t = t_1$, $|\phi\rangle$, related to the state at $t = t_2$, $|\phi'\rangle$ by $|\phi'\rangle = U|\phi\rangle$ where U is a unitary operator, that is $UU^\dagger = I$ where $U^\dagger$ is the Hermitian conjugate. The evolution can also be described by the Schrödinger equation,

$$i\hbar\frac{\mathrm{d}|\phi\rangle}{\mathrm{d}t} = \hat{H}|\phi\rangle, \tag{1.2}$$

where $\hbar$ is Planck's constant and $\hat{H}$ is a Hermition operator, i.e. $\hat{H} = \hat{H}^\dagger$, known as the Hamiltonian. There are two main interpretations of evolution, the Schrödinger picture and the Heisenberg picture. In the Schrödinger picture $\hat{H}$ is taken to evolve with time as the state vector does not. In the Heisenberg picture the state vector evolves with time and $\hat{H}$ does not. The Schrödinger picture is commonly used in to describe the evolution of discrete variable systems. For continuous variable systems the Heisenberg picture is used.

1.1.3 Measurement

The measurement of a quantum state can be described by a collection of measurement operators $\{\hat{M}_m\}$ where m is the index of the measurement outcomes. For example consider the qubit in Eq. (1.1) with the family of measurement operators $\hat{M}_0 = |0\rangle\langle 0|$ and $\hat{M}_1 = |1\rangle\langle 1|$. The operator $\hat{M}_0$ will measure if $|\phi\rangle = |0\rangle$ and similarly $\hat{M}_1$ will measure if $|\phi\rangle = |1\rangle$. Though in quantum mechanics a state is not predefined so the measurement operators will have a probability of the measurement return a result 0 or 1. These probabilities are given by,

$$p(0) = \langle\phi|\hat{M}_0^\dagger\hat{M}_0|\phi\rangle = |a|^2, \tag{1.3}$$

$$p(1) = \langle\phi|\hat{M}_1^\dagger\hat{M}_1|\phi\rangle = |b|^2. \tag{1.4}$$

After a measurement is made the state will change depending on the result and become,

$$\frac{\hat{M}_m|\phi\rangle}{\sqrt{\langle\phi|\hat{M}_m^\dagger, \hat{M}|\phi\rangle}} \tag{1.5}$$

For the above example if 0 is the measurement result the state will be $|0\rangle$ after the measurement and similarly the state will be $|1\rangle$ if 1 is measured.

Projective measurements

An equivalent description of the general measurement given above is the class of projective measurements. A projective measurement is described by a Hermition operator, $\hat{M}$, known as an observable. The observable can be decomposed into a linear combination of projectors, $\hat{P}_m$, into the eigenspace of $\hat{M}$,

$$\hat{M} = \sum_m m\hat{P}_m \tag{1.6}$$

The outcomes of a projective measurements will correspond to the eigenvalue, m, of $\hat{M}$. The probability of measuring the eigenvalue m is given by

$$p(m) = \langle\phi|\hat{P}_m|\phi\rangle \tag{1.7}$$

After measurement given m was measured the state will become,

$$\frac{\hat{P}_m|\phi\rangle}{\sqrt{p(m)}} \tag{1.8}$$

The expected value for a projective measurement is easily calculated as,

$$E(\hat{M}) = \langle\phi|\hat{M}|\phi\rangle \tag{1.9}$$

A common notation for the expected value is also $\langle\hat{M}\rangle$. The variance of an observable follows as,

$$\Delta^2(\hat{M}) = \langle\hat{M}^2\rangle - \langle\hat{M}\rangle^2 \tag{1.10}$$

1.1.4 Composite systems

A composite system can be formed with individual component systems. The state space for a composite system is described by the tensor product of the component systems state spaces. A state vector in a composite system with n component systems is then described by $|\phi_1\rangle\otimes|\phi_2\rangle\otimes\ldots|\phi_n\rangle$ where $|\phi_i\rangle$ is a state vector in the state space for the ith component system. The state vector is more commonly written as $|\phi_1\phi_2\ldots\phi_n\rangle$. An operator acting on the composite state space is also described by a tensor product of operators acting on the component state space.

Entanglement

An important example of a composite system is an entangled state. For a composite system made up of system A and system B both described by the qubit state space. Consider the state,

$$\frac{1}{\sqrt{2}}(|0_{\mathrm{A}}0_{\mathrm{B}}\rangle + |1_{\mathrm{A}}1_{\mathrm{B}}\rangle) \tag{1.11}$$

This state is interesting because a measurement performed on system A will project the state of system B regardless of how far apart they are. Measurement of both states will reveal correlations that forgo local realism as a physical law. This topic is explored further in Sec. 1.2 and Ch. 4. Consider the set of measurement operators, $\hat{M}_m = \hat{M}_m^{\mathrm{A}} \otimes \hat{I}^{\mathrm{B}}$ where $m = \{0, 1\}$, $\hat{M}_m^{\mathrm{A}}$ is defined in Sec. 1.1.3 and $\hat{I}^{\mathrm{B}}$ is the identity operator on the state space of system B. The projection of the state after measurement is given by,

$$\frac{\hat{M}_m|\psi\rangle}{\sqrt{\langle\psi|\hat{M}_m^\dagger\hat{M}_m|\psi\rangle}} = |m_{\mathrm{A}}m_{\mathrm{B}}\rangle \tag{1.12}$$

System B has been projected to either $|0\rangle$ or $|1\rangle$ depending on the outcome on the measurement of system A.

1.1.5 Density operators

A more general way to describe the state of a quantum system is with a density operator. For a pure quantum system the density operator is given by $\hat{\rho} = |\phi\rangle\langle\phi|$. If the density operator can be written in this way it is said to be in a pure state. Additionally a state is pure if and only if $\hat{\rho}^2 = \hat{\rho}$. Conversely a mixed state is one that cannot be represented by a simple state vector but can be represented by an ensemble of pure states,

$$\hat{\rho} = \sum_i p_i|\phi_i\rangle\langle\phi_i|. \tag{1.13}$$

The purity of a state can be measured by using the trace operator on the square of the density operator, $\mathrm{tr}(\hat{\rho}^2)$. The trace will give a value between $1/n$ and 1 with 1 representing a pure state and n being the dimension of the Hilbert space. A composite system can also be described by density operators for example a two mode state is represented as $\hat{\rho}_{\mathrm{AB}} = |\phi_{\mathrm{AB}}\rangle\langle\phi_{\mathrm{AB}}|$. The partial trace operation can be used to remove a system form a state,

$$\hat{\rho}_{\mathrm{AB}} \xrightarrow{\mathrm{PT}} \hat{\rho}_{\mathrm{A}}. \tag{1.14}$$

For this thesis density operators are not used in any meaningful way other than a convenient way to refer to a quantum state and in particular mixed states. A more complete description is given in Ref. [13].

1.2 Bell Tests

The Bell test is a fundamental demonstration of quantum mechanics. It is made up of a family of inequalities that test the hypothesis of local realism [22]. A violation of a Bell inequality by two spatially separated parties will demonstrate non local correlations between them which is an indication of quantum entanglement. The original idea of entanglement is know as the EPR Paradox [1]. The Authors of the EPR paradox conducted a thought experiment where two separated particles, A and B, that have previously interacted could from the measurement of the position of A, infer the position of particle B beyond the quantum limit without it being disturbed. The conclusion was that quantum mechanics at the time did not provide a complete description of reality. It was suggested that a hidden variable could be used to explain the paradox. John Bell explored the paradox and came up with a theorem that any local hidden variable model would be violated by the predictions of quantum mechanics [2]. To test this theorem many Bell inequalties have been proposed to bound results from a local hidden variable description of experimental results [22]. The most famous of them is the CHSH Bell inequality [23],

$$E(A,B) + E(A',B') + E(A',B) - E(A,B') \leq 2, \tag{1.15}$$

where $E(X,Y)$ is the expectation value of the random variables X and Y. A basic experiment can be constructed around Eq. (1.15) to demonstrate a violation. Consider the Fig. 1.1 where a source distributes a bipartite state between two non-local parties, Alice and Bob, each with their own measurement device. They can change their measurements to one of two observables, $\hat{A}$ and $\hat{A}'$ for Alice and $\hat{B}$ and $\hat{B}'$ for Bob. Each measurement will give the outcome ± 1. At a prearranged time Alice and Bob will each receive a state and perform a measurement with a randomly selected setting. The goal of Alice and Bob is to violate Eq. (1.15). A simple derivation of the CHSH inequality can be used to see how this protocol can violate Eq. (1.15) [13]. Suppose the state distributed to Alice and Bob obeys they theory of local realism, that is the joint state has a real physical property that exists independently of observation and Alice and Bob can only interact through local effects. For this derivation assume Alice and Bob can not influence each others measurements. Consider the quantity $AB + AB' + A'B' - A'B$ where A, A', B and B' represent the outcome from their respective measurements. With $A, A', B, B' = \pm 1$ it is easy to

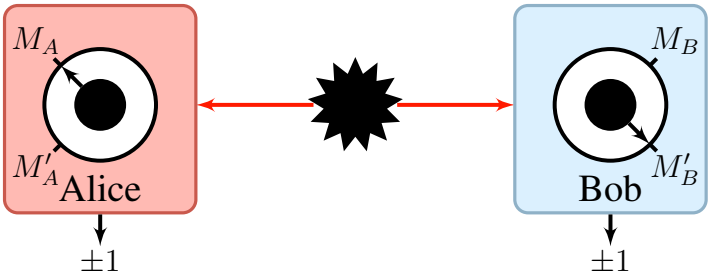


Figure 1.1: A source distributes a Bell state to Alice and Bob. Alice and Bob each have their own measurement apparatus that can perform one of two measurements. Comparing their measurements they can violate Eq. (1.15).

see that this quantity can only be ± 2. Now consider the mean value of this quantity,

$$E(AB + AB' + A'B' - A'B) = \sum_{aa'bb'} p(a, a', b, b')(ab + ab' + a'b' - a'b) \tag{1.16}$$

$$\leq \sum_{aa'bb'} p(a, a', b, b') \times 2 \tag{1.17}$$

$$= 2, \tag{1.18}$$

Where $p(a, a', b, b')$ is the probability of the joint state being predetermined prior to measurement such that the result will be $A = a$, $A = a'$, $B = b$ and $B' = b'$. Using the linearity of the expected value the CHSH inequality in Eq. (1.15) can be derived.

Now consider the quantum state

$$|\phi\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}. \tag{1.19}$$

Where the source distributes one mode to Alice and one to Bob. Using the observables,

$$\hat{A} = Z \qquad \hat{B} = \frac{-Z - X}{\sqrt{2}} \tag{1.20}$$

$$\hat{A}' = X \qquad \hat{B}' = \frac{Z - X}{\sqrt{2}}, \tag{1.21}$$

with $X = |0\rangle\langle 0| + |1\rangle\langle 1|$ and $Z = |0\rangle\langle 0| - |1\rangle\langle 1|$. The expectation values are;

$$E(\hat{A}, \hat{B}) = \frac{1}{\sqrt{2}}, \quad E(\hat{A}', \hat{B}) = \frac{1}{\sqrt{2}}, \quad E(\hat{A}', \hat{B}') = \frac{1}{\sqrt{2}}, \quad E(\hat{A}, \hat{B}') = -\frac{1}{\sqrt{2}}. \tag{1.22}$$

Interestingly this gives,

$$E(\hat{A}, \hat{B}) + E(\hat{A}', \hat{B}) + E(\hat{A}', \hat{B}') - E(\hat{A}, \hat{B}') = 2\sqrt{2}. \tag{1.23}$$

A clear violation of the original inequality and a demonstration that with quantum mechanics nature does not obey local-realism. The value of $2\sqrt{2}$ is known as the Tsirelson's bound. This is the largest possible violation with the CHSH inequality [24].

In the derivation above it was assumed that Alice and Bob could not interact and every measurement yielded a result. This of course is not realistic to experiments and there are several loopholes [22] that can cause a violation of a Bell inequality. The most obvious is communication between Alice and Bob which can easily violate Eq. (1.15). This is knowm as the locality loophole. For example every time Alice decides a measurement she could tell the Bob and cause fake Bell violations. This is easily solved in optics experiments where Alice and Bob are moved far enough apart that even with speed of light communication they cannot exchange any relevant information in the time it takes to perform a measurement [25]. Another common loophole comes from the measurement process. A realistic measurement will have some loss associated with it. This loss results in a third possible outcome from the measurement being a "no click" or 0. These "no clicks" can be discarded but there is a threshold of measurement efficiency below of which a violation can be faked [26]. This is known as the detection loophole or the fair sampling assumption as the recorded data has to be representative of the distributed state.

There have been a number of experiments dating back over 35 years [3] that have demonstrated a violation of a Bell inequality but only recently has it been possible to overcome both the detection and locality loopholes. There have so far been four experiment where a convincing violation has been produced [4–7]. Each of these experiments employed high efficiency detection methods to address the detection loophole and careful analysis of the separation of Alice and Bob to address the locality loophole. Each measurement setting was also chosen at random using a mixture of several sources of random numbers including quantum random number generators (QRNG). These experiments have opened up the possibility for practical applications of Bell tests in quantum technology where one is faced with the question of verification of quantum devices. For quantum key distribution (QKD) and QRNGs, a violation of a Bell inequality can rule out any tampering of the quantum source or the measurement devices. This allows the user to achieve device independent (DI) protocols [18].

1.3 Quantum states of light

So far only the mathematical description of a qubit has been considered. The system of interest for this thesis is the electric field of an optical field. In this section a number of experimentally realisable optical states that are used throughout this thesis will be described. Following from Ref. [27] and Ref. [19], quantum field theory gives the vector potential of

an optical field as,

$$\hat{\boldsymbol{A}}(\boldsymbol{r},t)=\sum_{k}\left(\frac{\hbar}{2\omega_k\varepsilon_0}\right)\left[\hat{a}_k\mathbf{u}_k(\mathbf{r})e^{-i\omega_k t}+\hat{a}_k^{\dagger}\mathbf{u}_k^{*}(\mathbf{r})e^{i\omega_k t}\right] \tag{1.24}$$

where the vector $\boldsymbol{k}$ is the propagation vector, ω is the angular frequency of the field, $\boldsymbol{A}_0$ is a complex vector potential orthogonal to $\boldsymbol{k}$ and $\hat{a}$ is the annihilation operator with its Hermitian conjugate, $\hat{a}^{\dagger}$ the creation operator. The vector potential can be written as a sum of modes, i.e. subsystems, denoted by the subscript k. For each mode the annihilation and creation operators obey the following bosonic commutation relations, where $\mathbf{u}_k$ are vector mode functions corresponding to a mode with an angular frequency ω_k and $\hat{a}$ is the annihilation operator with its Hermitian conjugate, $\hat{a}^{\dagger}$ the creation operator. The vector mode functions define the direction of travel in the case of a traveling wave. The vector potential can be written as a sum of modes, i.e. subsystems, denoted by the subscript k. For each mode the annihilation and creation operators obey the following bosonic commutation relations,

$$[\hat{a}_k,\hat{a}_k']=[\hat{a}_k^{\dagger},\hat{a}_k'^{\dagger}]=0 \qquad \text{and} \qquad [\hat{a}_k,\hat{a}_k'^{\dagger}]=\delta_{kk'}, \tag{1.25}$$

From Eq. (1.24) the electric field operator, $\hat{\boldsymbol{E}}(\boldsymbol{r},t)$, and the magnetic flux density operator, $\boldsymbol{B}(\boldsymbol{r},t)$, can be found using,

$$\hat{\boldsymbol{B}}=\nabla\times\hat{\boldsymbol{A}} \qquad \hat{\boldsymbol{E}}=-\frac{\partial\hat{\boldsymbol{A}}}{\partial t}. \tag{1.26}$$

This gives the electric field operator,

$$\hat{\boldsymbol{E}}(\boldsymbol{r},t)=i\sum_{k}\left(\frac{\hbar\omega_k}{2\varepsilon_0}\right)^{\frac{1}{2}}\left[\hat{a}_k\boldsymbol{u}_k(\boldsymbol{r})e^{-i\omega_k t)}-\hat{a}^{\dagger}\boldsymbol{u}^{*}(\boldsymbol{r})e^{i\omega t)}\right]. \tag{1.27}$$

The Hamiltonian of electromagnetic field can be found using,

$$\hat{H}=\frac{1}{2}\int(\varepsilon_0\hat{\boldsymbol{E}}(\boldsymbol{r},t)\cdot\hat{\boldsymbol{E}}(\boldsymbol{r},t)+\frac{1}{\mu_0}\hat{\boldsymbol{B}}(\boldsymbol{r},t)\cdot\hat{\boldsymbol{B}}(\boldsymbol{r},t))\mathrm{d}\boldsymbol{r} \tag{1.28}$$

$$=\sum_{k}\hbar\omega_k\left(\hat{a}_k^{\dagger}\hat{a}_k+\frac{1}{2}\right). \tag{1.29}$$

Which is the Hamiltonian of a simple harmonic oscillator. The two terms that appear in the Hamiltonian are the photon number operator defined as $\hat{n}=\hat{a}^{\dagger}\hat{a}$ multiplied by the energy in each photon and a vacuum energy term $\frac{1}{2}\hbar\omega$. That is the energy that exists in a vacuum even without the presence of an optical field. It is the manipulation of the vacuum

modes that forms the basis for this thesis.

The significance of the number operator comes from it being observable with the discrete eigenstates,

$$\hat{n}|n\rangle = n|n\rangle, \tag{1.30}$$

where $n \in \mathbb{N}$. Two other observable operators are given by the natural analogue to the position and momentum, the amplitude, $\hat{x}$ and phase $\hat{p}$ operators. These operators are continuous variable observables and are defined in terms of the annihilation and creation operators,

$$\hat{x} = \sqrt{\frac{\hbar}{2\omega}}(\hat{a} + \hat{a}^\dagger) \tag{1.31}$$

$$\hat{p} = i\sqrt{\frac{\hbar\omega}{2}}(\hat{a} - \hat{a}^\dagger), \tag{1.32}$$

with the commutation relation,

$$[\hat{x}, \hat{p}] = i\hbar. \tag{1.33}$$

These can be considered in some sense to be the real and imaginary part of the annihilation operator [27]. The eigenstates for the quadrature variables are not physically realisable but are given by,

$$\hat{x}|x\rangle = x|x\rangle \qquad \text{and} \qquad \hat{p}|p\rangle = p|p\rangle, \tag{1.34}$$

where x and p are continuous variables. That is $x \in \mathbb{R}$ and $p \in \mathbb{R}$ [8, 28]. Making $\hat{x}$ and $\hat{p}$ the continuous variable observables. Using the quadrature operators the electric field operator for a single mode can be rewritten in the form,

$$\hat{E}(\boldsymbol{r}, t) = \left(\frac{\hbar\omega}{2\varepsilon}\right)^{\frac{1}{2}} \left[\hat{x}\sin(\omega t - \boldsymbol{k}\cdot\boldsymbol{r}) - \hat{p}\cos(\omega t - \boldsymbol{k}\cdot\boldsymbol{r})\right], \tag{1.35}$$

where $\boldsymbol{k}$ is the direction vector of the field. Unsurprisingly the quadrature operators act as the amplitude operators on the phase and quadrature components of the electric field. As the operators $\hat{x}$ and $\hat{p}$ are non commuting observables the Heisenberg uncertainty principle (HUP) places a lower bound on the uncertainty of these two operators with,

$$\Delta A \Delta B \geq \frac{1}{2}|\langle[A, B]\rangle|. \tag{1.36}$$

Using the phase and quadrature operators this becomes,

$$\Delta\hat{x}\Delta\hat{p} \geq \frac{1}{2}|\langle[\hat{x}, \hat{p}]\rangle| = \frac{1}{2}\hbar \tag{1.37}$$

It is convenient for the remainder of this thesis to take $\hbar = 2$ and $\omega = 1$ to simplify the description of quantum states. This simplifies the uncertainty principle to,

$$\Delta\hat{x}\Delta\hat{p} \geq 1 \tag{1.38}$$

1.3.1 The Fock states

While it is not widely used in this thesis it is useful to know about the Fock basis. The Fock basis is made up by the eigenstates of the number operator. A Fock state is represented by the vector $|n\rangle$ where n is the number of photons in an optical field. The Fock basis can be used to make optical qubits. The action of the creation, annihilation and number operators on a Fock state is,

$$\hat{a}^\dagger|n\rangle = \sqrt{n+1}|n+1\rangle, \qquad \hat{a}|n\rangle = \sqrt{n}|n-1\rangle \quad \text{and} \quad \hat{n}|n\rangle = n|n\rangle. \tag{1.39}$$

The minimum energy state or vacuum state is denoted by $|0\rangle$ and is defined by

$$\hat{a}|0\rangle = 0 \tag{1.40}$$

with the expected value of this state given by,

$$\langle 0|\hat{n}|0\rangle = 0. \tag{1.41}$$

All Fock states are accessible from the repeated application of the creation operator. The Fock basis forms a complete basis and every state is orthogonal,

$$\sum_{n=0}^{\infty} |n\rangle\langle n| = 1, \qquad \langle n|m\rangle = \delta_{mn}. \tag{1.42}$$

1.3.2 Coherent states

The coherent states are interesting as they are minimum uncertainty states and are the closest quantum states to a classical description of an optical field. The significance of these states is they are the natural state generated by a shot noise limited laser. These states are created by the application of the displacement operator on a vacuum state. The displacement operator is given by [19],

$$\hat{D}(\alpha) = \exp\left(\alpha\hat{a}^\dagger - \alpha^*\hat{a}\right), \tag{1.43}$$

A coherent state, $|\alpha\rangle$, can be written in the Fock basis as,

$$|\alpha\rangle = \hat{D}(\alpha)|0\rangle = e^{-|\alpha|^2/2} \sum_n \frac{\alpha^n}{\sqrt{(n!)}} |n\rangle. \tag{1.44}$$

The coherent state has a indefinite number of photons. The probability distribution of the Fock states in a coherent state is Poisson,

$$P(n) = |\langle n|\alpha\rangle|^2 = \frac{|\alpha|^{2n} e^{-|\alpha|^2}}{n!}. \tag{1.45}$$

Unlike Fock states coherent states are not orthogonal to each other and form an over complete basis,

$$\langle \beta|\alpha\rangle = \exp\left[-\frac{1}{2}(|\alpha|^2 + |\beta|^2) + \alpha\beta^*\right] \tag{1.46}$$

The variance of the quadrature operators of a coherent state are given by,

$$\Delta\hat{x} = 1, \qquad \Delta\hat{p} = 1 \tag{1.47}$$

A coherent state is part of a family of minimum uncertainty states which achieve the HUP lower bound,

$$\Delta x \Delta p = 1 \tag{1.48}$$

A simple illustration of a coherent state can be made by a ball and stick diagram as shown in Fig. 1.2 (a). The uncertainty of the state is represented by a ball of radius 1 which is centered at $\alpha = \langle \hat{x} + i\hat{p}\rangle$.

1.3.3 Squeezed states

A more general minimum uncertainty state is the squeezed state. The defining feature of a squeezed state is the unequal uncertainty in each quadrature. A squeezed coherent state can be generated first by applying the squeezing operator $S(\varepsilon)$, with a squeezing parameter of $\varepsilon = re^{2i\phi}$, and then the displacement operator to a vacuum state. The squeezing operator is given by [19],

$$\hat{S}(\varepsilon) = \exp\left(\frac{1}{2}(\varepsilon^* \hat{a}^2 - \varepsilon \hat{a}^{\dagger 2})\right). \tag{1.49}$$

The squeezing operator applied to a coherent state, Fig. 1.2 (b), results in a scaling of the quadratures parameterized by the squeeze factor, r, and a rotation by ϕ. A squeezed state

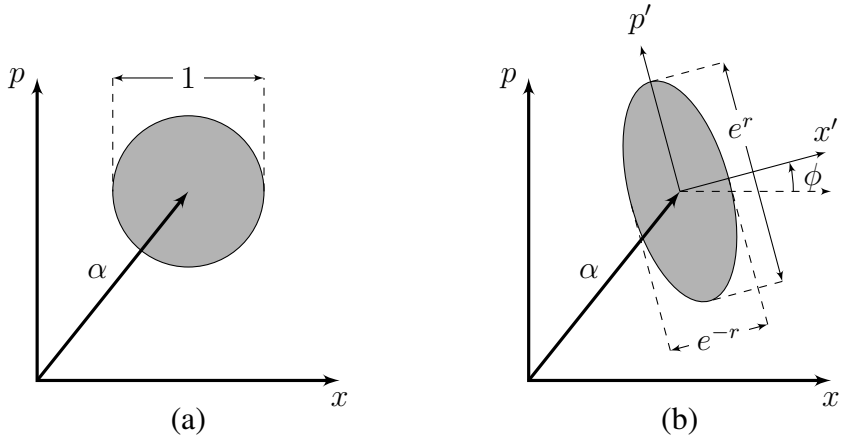


Figure 1.2: A ball and stick diagram. The uncertainty of a coherent state, (a), is represented by a ball centered at $\frac{1}{2}\langle x + ip\rangle = \alpha$. A squeezed state, (b), is scaled by e^{-r} in the x quadrature and e^{r} in the p quadrature and rotated by ϕ.

is also a minimum uncertainty state with the variance of the rotated quadrature given by

$$\Delta x = e^{-r} \qquad \Delta p = e^{r}. \tag{1.50}$$

The photon number distribution for a squeezed state is given by,

$$P(n) = \frac{\left(\frac{1}{2}\tanh(r)\right)^{n}}{n!\cosh(r)} \exp\left[-|\alpha|^2 - \frac{1}{2}\tanh(r)\left((\alpha^*)^2 e^{i\phi} + \alpha^2 e^{-i\phi}\right)\right] |H_n(z)|^2, \tag{1.51}$$

where,

$$z = \frac{\alpha + \alpha^2 e^{i\phi}\tanh(r)}{\sqrt{2e^{i\phi}\tanh(r)}}, \tag{1.52}$$

and $|H_n(z)|$ is the nth Hermite polynomial. It is interesting to note that $H_n(0) = 0$ for odd values of n. Operationally this means that squeezed vacuum states only contain even numbered Fock states. When the squeezing operator is used on a coherent state the probability distribution Eq. (1.51) will widen if $r < 0$ or narrow if $r > 0$. For large values of r the probability distribution will oscillate at higher photon numbers. The probability distribution for the case of low r is plotted in Fig. 1.3.

Experimentally a squeezed state can be generated through a process called optical parametric amplification (OPA) where a non-linear crystal is pumped by the second harmonic of the fundamental mode. The term r is proportional to the non-linear interaction between the second harmonic and the fundamental fields. The angle ϕ is the phase between the pump and fundamental fields. This process is described in Ch. 2 with some experiment results presented Ch. 3.

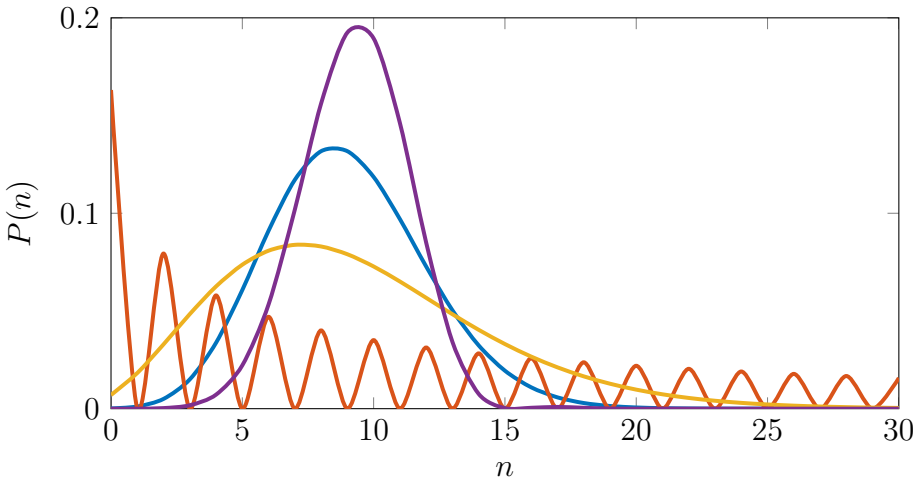


Figure 1.3: The photon number distribution for a coherent state (blue) with $\alpha = 3$, a phase squeezed coherent state (yellow) with $\alpha = 3$ and $r = -0.5$, an amplitude squeezed coherent state (purple) with $\alpha = 3$ and $r = 0.5$ and a vacuum squeezed state (red) with $r = 2.5$.

1.3.4 Thermal states

It is sometimes useful for the description of a quantum system to consider non-minimum uncertainty Gaussian states called thermal states. A thermal state is a mixed state that describes the field emitted by a black body. The density operator for this state using the Fock basis is given by [29],

$$\hat{\rho} = \frac{1}{1+\bar{n}} \sum_{n=0}^{\infty} \left(\frac{\bar{n}}{1+\bar{n}} \right)^n |n\rangle\langle n|, \tag{1.53}$$

where $\bar{n}$ is the mean photon number in the field. The variance of the thermal states in the quadratures is given by $\Delta^2 x = \Delta^2 p = 2\bar{n} + 1$.

1.3.5 Two important unitary operators

The states discussed in Sec. 1.3 can be used in combination with other states using unitary operators. This section will cover two important operations for this thesis, the beam splitter operation and the phase shift operation.

Phase shift

The phase shift operator is parameterised by the variable θ. The transformation acting on field $\hat{a}_{\text{in}}$ is simply,

$$\hat{U}_{\text{PS}}(\theta) = e^{-i\theta\hat{n}} \tag{1.54}$$

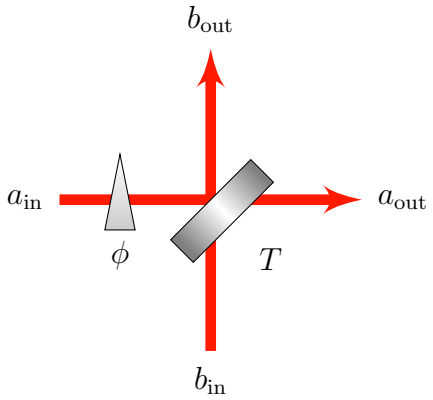


Figure 1.4: The optical fields $\hat{a}_{\text{in}}$ and $\hat{b}_{\text{in}}$ combined on a beam splitter of transmission T. Mode $\hat{a}_{\text{in}}$ is shifted in phase by ϕ relative to $\hat{b}_{\text{in}}$

The phase shift operator represents a rotation in the quadratures of an optical field,

$$\hat{x}_\theta \hat{U}_{\text{PS}}(\theta)\hat{x}\hat{U}^\dagger_{\text{PS}}(\theta) = \cos(\theta)\hat{x} + \sin(\theta)\hat{p} = \hat{a}e^{-i\theta} + \hat{a}^\dagger e^{i\theta} \tag{1.55}$$

Beam splitter

A beam splitter is one of the more basic elements and most common of any optics experiment that is used to combine or split beams through a semitransparent surface with a transmission $0 \leq T \leq 1$ and reflectivity $R = 1 - T$. In quantum optics a beam splitter is always considered a four port device. A beam splitter can be combined with the phase shift operator to control which quadratures will interfere. Consider a beam splitter with a transmission of T acting on two optical fields $\hat{a}_{\text{in}}$ and $\hat{b}_{\text{in}}$ the transformation is given by,

$$\begin{bmatrix} \hat{a}_{\text{out}} \\ \hat{b}_{\text{out}} \end{bmatrix} = \begin{bmatrix} \sqrt{T} & \sqrt{1-T} \\ -\sqrt{1-T} & \sqrt{T} \end{bmatrix} \begin{bmatrix} e^{-i\phi}\hat{a}_{in} \\ \hat{b}_{in} \end{bmatrix}, \tag{1.56}$$

where $e^{-i\phi}$ is a phase shift acting on mode $\hat{b}_{in}$. A simple illustration of a beam splitter is given in Fig. 1.4.

The beam splitter operator is significant in experimental modeling as it provides a way to model experiment losses. All experimental processes will experience some kind of loss. These include spatial mode matching, inefficient detection and scattering from optical components. The beam splitter operator can be used to model loss, and the coupling of a vacuum or a thermal state from the environment into the signal mode. In this thesis the second mode produced is considered destroyed, and the mode is traced out of the state. In the context of Fig. 1.4 if mode $\hat{a}_{\text{in}}$ is the signal then mode $\hat{b}_{\text{in}}$ is the environment noise and mode $\hat{b}_{\text{out}}$ is thrown away

1.3.6 Two mode squeezed states

The name two mode squeezed state gets comes from the property that the squeezing is now over two modes. Through this thesis they are commonly referred to as entangled states or EPR states. In this thesis an entangled state is generated from two squeezed vacuum states mixed in quadrature on a beam splitter with $T = 0.5$. The combination of the two squeezing operators and the beam splitter results in the two mode squeeze operator given by,

$$\hat{S}(G) = \exp\left(G^* \hat{a}_{\mathrm{A}} \hat{a}_{\mathrm{B}} - G \hat{a}_{\mathrm{A}}^{\dagger} \hat{a}_{\mathrm{B}}^{\dagger}\right), \tag{1.57}$$

where $G = re^{-i\theta}$. This operator can be used to describe the generation of two entangled modes of different frequencies, ω_{A} and ω_{B}. For this thesis the modes A and B will be spatially separated. It is interesting to note that each mode in a two mode squeezed state has the quadrature variance $\Delta^2 \hat{x} = \Delta^2 \hat{p} = \cosh(r)$. Meaning the modes individually are thermal states. The squeezing exists in the correlation between the two modes.

1.4 Phase-space representation

An alternative to describing a quantum state with a density operator is to use a Wigner function. The Wigner function is a quasiprobability distribution defined over a real symplectic space [28]. The Wigner function is outside the scope of this thesis but a comprehensive description can be found in Ref. [30]. What is of interest here though is that the Wigner function can be described by the moments of the quantum state.

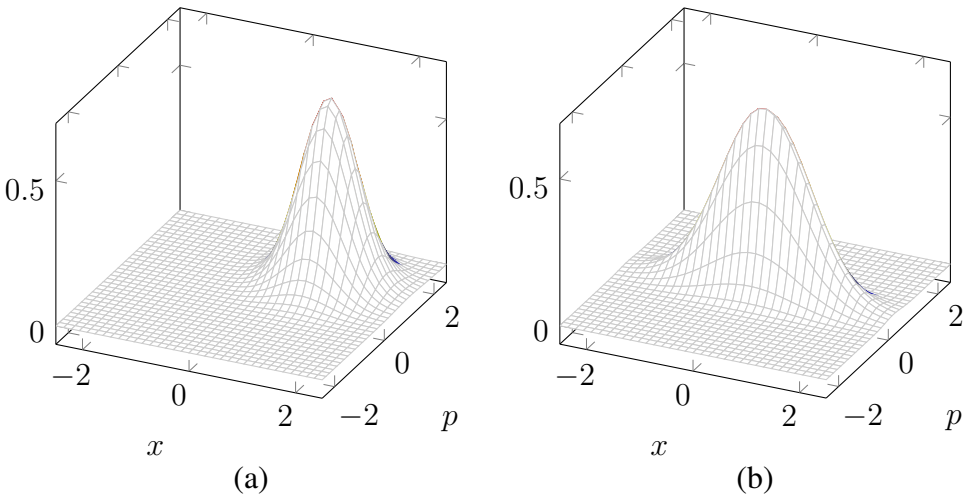


Figure 1.5: Examples of a Wigner function for a coherent state, (a), and a squeezed state, (b), where $\alpha = 1 + i$ and $r = 0.5$.

The coherent, squeezed, two mode squeezed states and thermal states are part of a

family of Gaussian states that can be completely described by their variance and mean in the phase and amplitude quadratures [29]. The covariance matrix and mean vector for a vacuum state is given by,

$$\gamma = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad d = \begin{bmatrix} 0 \\ 0 \end{bmatrix}. \tag{1.58}$$

Here element $\gamma_{(1,1)}$ and d_1 represent the variance and mean respectively of the state in the x quadrature. Likewise for elements $\gamma_{(2,2)}$ and d_2 in the p quadrature. Just as was shown in Sec. 1.3 and Sec. 1.1.4 each of the minimum uncertainty states can be found by using an operator on the vacuum state. The covariance matrix for the single mode states is given by,

$$\gamma = \begin{bmatrix} \Delta^2 x & 0 \\ 0 & \Delta^2 p \end{bmatrix} \qquad d = \begin{bmatrix} \langle x \rangle \\ \langle p \rangle \end{bmatrix}. \tag{1.59}$$

The purity of a state described by a covariance matrix is given by $\frac{1}{2\sqrt{\gamma}}$ [31].

1.4.1 Composite systems

Multiple modes in a state can be represented by a single covariance matrix and mean vector. For N modes this would look like,

$$\gamma = \begin{bmatrix} \gamma_1 & \cdots & C_{1,N} \\ \cdots & \ddots & \vdots \\ C_{N,1} & \cdots & \gamma_N \end{bmatrix} \qquad \text{and} \qquad d = \begin{bmatrix} d_1 \\ \vdots \\ d_N \end{bmatrix}, \tag{1.60}$$

where each element γ_n and $C_{n,m}$ represents a 2×2 diagonal matrix, d_n is a 2 element vector with $n, m = \{0, 1, \ldots, N\}$. The sub matrix $C_{n,m}$ will represent the correlations between modes n and m. A partial trace of a Gaussian composite system will remove an element from the covariance matrix and mean vector. Consider a partial trace on a bipartite system, ρ_{AB} to trace out mode B. The covariance matrix will become,

$$\gamma_{\mathrm{AB}} = \begin{bmatrix} \gamma_{\mathrm{A}} & C \\ C & \gamma_{\mathrm{B}} \end{bmatrix} \xrightarrow{\mathrm{PT}} \gamma_{\mathrm{A}} \tag{1.61}$$

and the mean vector,

$$d_{\mathrm{AB}} = (d_{\mathrm{A}}, d_{\mathrm{B}}) \xrightarrow{\mathrm{PT}} d_{\mathrm{A}} \tag{1.62}$$

1.4.2 Gaussian operations

A Gaussian operator simply maps a Gaussian state to another Gaussian state. The corresponding operators for each of the operators given in Sec. 1.3 and Sec. 1.1.4 are given here.

Displacement operator

The displacement operator used to generate coherent states simply translates the mean of the state, $d_{\text{out}} = d_{\text{in}} + z$, where z is the displacement in the x and p quadrature. The covariance matrix under the displacement operator is invariant.

Symplectic transform

Any unitary operator U_S will have a corresponding symplectic operation S due to the Stone-von Neumann theorem. A symplectic transformation applied with the mapping,

$$d_{\text{out}} = S d_{\text{in}} \qquad \gamma_{\text{out}} = S \gamma_{\text{in}} S^T, \tag{1.63}$$

where S is $2N \times 2N$ matrix with real elements. The symplectic operation for the passive operations described in Sec. 1.3 are given below

Phase shift A phase shift of a mode by θ is simply a rotation between the quadratures. The symplectic operator for a single mode state is given by,

$$S_{\text{PS}}(\theta) = \begin{bmatrix} \cos(\theta) & \sin(\theta) \\ -\sin(\theta) & \cos(\theta) \end{bmatrix}. \tag{1.64}$$

Beam splitter A beam splitter with transmission T acts on two modes with the sympletic operator,

$$S_{BS}(T) = \begin{bmatrix} \sqrt{T}\mathbb{I} & \sqrt{1-T}\mathbb{I} \\ -\sqrt{1-T}\mathbb{I} & \sqrt{T}\mathbb{I} \end{bmatrix} \tag{1.65}$$

Squeezing operator The symplectic operator to squeeze a single mode state is given by,

$$S_{Sq}(r) = \begin{bmatrix} e^{-r} & 0 \\ 0 & e^{r} \end{bmatrix} \tag{1.66}$$

The unitary squeezed state operator also acted as a phase shift on the input state. To capture this the operator Eq. (1.66) can be combined with Eq. (1.64).

Two mode squeezed states The sympetic operators can be combined to create any Gaussian state. An important example for this thesis of this is generating an entangled state. As stated in Sec. 1.3.6 a two mode squeezed state can be created by combining two orthogonally squeezed states with a beam splitter. This gives the sympletic operator,

$$S_{BS}(\frac{1}{2})S^{\mathrm{A}}_{Sq}(r)S^{\mathrm{B}}_{Sq}(-r) = \begin{bmatrix} \cosh(r)\mathbb{I} & \sinh(r)\sigma_z \\ \sinh(r)\sigma_z & \cosh(r)\mathbb{I} \end{bmatrix}, \tag{1.67}$$

where the super script represents the mode being acted on by the operator and,

$$\sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \tag{1.68}$$

1.4.3 CP Maps

Not all desired transformations are unitary and covered by symplectic transformations. The family of completely positive maps (CP map) can be used to perform irreversible operations such as loss and is defined by two matrices X and Y applied to the covariance matrix and mean vector by,

$$\gamma_{\mathrm{out}} = X\gamma_{\mathrm{in}}X^T + Y \qquad d_{\mathrm{out}} = Xd_{\mathrm{in}} \tag{1.69}$$

Gaussian loss channel

A Gaussian loss channel can be modelled using a CP map with,

$$X = \sqrt{T}\mathbb{I} \qquad \text{and} \qquad Y = (1 - T + T\xi)\mathbb{I}, \tag{1.70}$$

where ϵ represents the noise in the channel relative to the input. This map is equivalent to mixing a state γ_{A} and a thermal state with a variance $1 + \frac{T}{1-T}\xi$.

Chapter 2

Experimental Techniques

2.1 Detecting quantum states

In Ch. 1 the electric field was written as a discrete mode. To make sense of the detection of quantum states a continuum of frequency modes must be considered. A multimode system can be made by taking a sum of modes each with an angular frequency ω_k and propagation vector $\boldsymbol{k}$. A continuum of modes can be made by considering the limit where the separation between the modes goes to 0. This creates new annihilation and creation operators which are related to the discrete operators by,

$$a \to \sqrt{\Delta\omega}a(\omega) \qquad \text{and} \qquad a^\dagger \to \sqrt{\Delta\omega}a^\dagger(\omega) \tag{2.1}$$

Understanding the continuum of modes is not essential to understand the work in this thesis. It is mentioned here to make the reader aware of the underlying description of sideband modes. For the work in this thesis, the modes discussed can be considered to be as described in Sec. 1.3. A rigorous description of this formalism for the continuum of modes is given Ref. [32, 33] and a more accessible description in Ref. [34]. The commutation relation for the new operators is now given by,

$$[a(\omega), a^\dagger(\omega')] = \delta(\omega - \omega'), \tag{2.2}$$

where $\delta(\omega - \omega')$ is the Dirac delta-function. The operators $\hat{x}(\omega)$ and $\hat{p}(\omega)$ are defined in a similar way to their discrete equivalents. The measurement of the observable operators are made relative to a carrier frequency, Ω, through the time varying field annihilation operator,

$$\tilde{a}(t) = \int_{-\Omega}^{\infty} \hat{a}_{\Omega+\omega}(\omega)e^{i\omega t}\mathrm{d}\omega, \tag{2.3}$$

where ω is the separation from the carrier frequency and decoration, $\tilde{}$, represents that the operator is in the time domain. The frequency domain annihilation operator can be

extracted from the time domain using the Fourier transform, denoted by $\mathbb{F}$, for $\omega < \Omega$,

$$\hat{a}(\omega) = \mathbb{F}(\tilde{a}(t)) \tag{2.4}$$

Similarly the same relation exists for the quadrature operators to move from the time domain operator to the frequency domain. Measuring the modes relative to a carrier frequency is more widely known as the rotating wave approximation.

2.1.1 Phase and Amplitude modulations

Only phase modulations are used in this thesis however amplitude modulations can be described in a similar way. The phase modulations are used to make error signals and control phase and cavity lengths. They can also be used together with amplitude modulations as the displacement operator for side band modes. There are two different types of devices used for phase modulation in this thesis. For low modulation frequencies, typically below 100kHz, Piezo driven mirrors are used. For large modulation frequencies, typically above 1MHz, electro-optic modulators are used. These modulators apply an electric field to a crystal to change its refractive index. The modulation of an optical field in the time domain relative to the carrier frequency is given by,

$$\tilde{a}_{\mathrm{PM}} = \tilde{a} e^{i\xi \cos(\omega_m t)}, \tag{2.5}$$

where $0 \geq \xi \leq 1$ is the modulation depth and ω_m is the modulation frequency. A modulation of ω_m will results in a number of harmonics being generated at integer multiples of ω_m with an amplitude that decays with the order of the harmonic. Assuming a small modulation depth the phase modulated field can be approximated by,

$$\tilde{a}_{\mathrm{PM}} \approx \tilde{a}\left(1 + i\frac{\xi}{2}e^{i\omega_m t} + i\frac{\xi}{2}e^{-i\omega_m t}\right). \tag{2.6}$$

The action of modulation is to move power from the carrier frequency, Ω, into the positive and negative sidebands $\Omega \pm \omega_m$. In the Fourier domain the modulation is given by,

$$\hat{a}_{\mathrm{PM}} = \mathbb{F}(\tilde{a}_{\mathrm{PM}}) \tag{2.7}$$

$$= \hat{a} + i\frac{\xi}{2}\hat{a}(\omega - \omega_m) + i\frac{\xi}{2}\hat{a}(\omega + \omega_m) \tag{2.8}$$

Phase modulation can be represented in a phasor diagram as illustrated relative to the carrier frequency in Fig. 2.1.

Amplitude modulation can be modeled in a similar way. An amplitude modulated

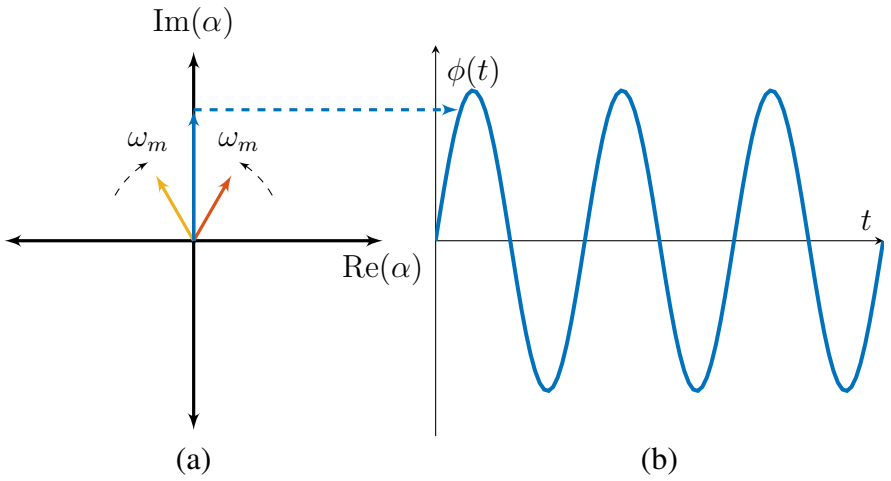


Figure 2.1: A phasor diagram, (a), showing the upper (red) and lower (yellow) sidebands rotating in opposite directions at a frequency of ω_m relative to the carrier. The two sidebands beat to create a phase modulation (blue) of the carrier, (b).

field relative to the carrier frequency is given by,

$$\tilde{a}_{\mathrm{PM}} = \tilde{a}(1 + \xi \cos(\omega_m t)). \tag{2.9}$$

With the Fourier transform given by,

$$\hat{a}_{\mathrm{AM}} = \hat{a} + \frac{\xi}{2}\hat{a}(\omega - \omega_m) + \frac{\xi}{2}\hat{a}(\omega + \omega_m) \tag{2.10}$$

2.1.2 Photodiode

A photodiode is a device that converts an optical field to a current using the photoelectric effect. The current produced is proportional to the photon number operator for the field [8, 19],

$$i_d(t) \propto \tilde{a}^\dagger \tilde{a}. \tag{2.11}$$

To make sense of the diode current it is beneficial to consider the linearised decomposition of the annihilation and creation operators,

$$\tilde{a} = \alpha + \delta\tilde{a} \qquad \text{and} \qquad \tilde{a}^\dagger = \alpha^* + \delta\tilde{a}^\dagger, \tag{2.12}$$

where $\alpha = \langle \tilde{a} \rangle$ is the coherent amplitude of the laser and a fluctuating term $\delta\tilde{a}$. This linearization is made with the assumption that $\langle \delta\tilde{a} \rangle = 0$ and $|\langle \delta\tilde{a}^\dagger \delta\tilde{a} \rangle| \ll \alpha$. For the remainder of this thesis α is taken to be real. A detailed decription of the linearization is

made in Ref. [35]. With linearization of the operators the photodiode current becomes,

$$i_d(t) \propto \alpha^2 + \alpha\tilde{x}. \tag{2.13}$$

Moving to the frequency domain and restricting the analysis to the frequency bands with no significant noise, the photocurrent can be written as upper and lower sidebands similar to the classical phase modulation. The upper, $\Omega + \omega$ and lower $\Omega - \omega$ sidebands are given by,

$$i_d(\omega) = i(\omega) + i(-\omega) \propto \alpha(\hat{x}(\omega) + \hat{x}(-\omega)) \tag{2.14}$$

Experimentally the isolation of the sidebands in the detector current is made by using a combination of low and high pass electronic filters.

Photodetector

In an experiment the photodiode is used in a photodetector where the current is converted to a voltage using a transimpedance amplifier with some gain g_d. A basic circuit of a transimpedance amplifier can be found in App. A.1. The conversion of current to voltage can be done with a simple resister however for large gains this presents as a large impedance which reduces the signal to noise ratio. A transimpedance amplifier on the other hand presents as a low impedance load to the diode current through the use of an op amp for large gains [36].

2.1.3 Homodyne detection

The intensity can be easily measured using a single photodiode but to measure an arbitrary quadrature a homodyne detector is required. A homodyne detector works by interfering on a 50/50 beamsplitter a signal field, $\hat{a}$, with a stronger local oscillator field, $\hat{a}_{\mathrm{LO}}$ with some relative phase θ between the two input fields. The strength of the local oscillator needs to be such that $\alpha_{\mathrm{LO}} \gg \alpha$. Taking the difference between the two photocurrents as depicted in Fig. 2.2 measures the quadrature $\hat{x}^{\theta}$. The resulting measurement is amplified by the intensity of the local oscillator making it easier to measure weak quantum fluctuation in both quadratures. Using the linearisation of both fields the detected photocurrent is given by,

$$i_{\mathrm{diff}}(t) \approx g_{\mathrm{D}} \left[2\cos(\theta)\tilde{a}\alpha_{\mathrm{LO}} + \alpha_{\mathrm{LO}}(\delta\tilde{x}\cos(\theta) + \delta\tilde{p}\sin(\theta))\right] \tag{2.15}$$

The terms not containing α_{LO} are approximately 0. Taking the Fourier transform of $i_{\text{diff}}(t)$ the sideband mode can be written as,

$$i_{\text{diff}}(\omega) = g_D \alpha_{\text{LO}} (\delta\tilde{x}\cos(\theta) + \delta\tilde{p}\sin(\theta)) \tag{2.16}$$

For the quadrature measurement to make any sense it needs to be normalized to shot noise which can be measured by blocking mode a. For this thesis the normalization is such that the variance of the shot noise is one. For a state containing multiple correlated modes a

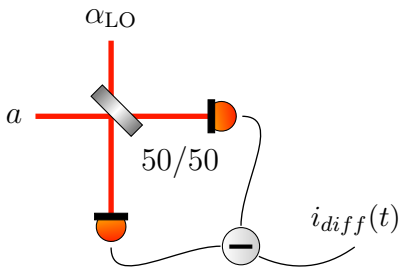


Figure 2.2: A homodyne detector. The signal beam is interfered on a 50/50 BS. Both ports of the BS are measured and the photocurrents subtracted to get i_{diff}.

homodyne measurement acts as a projective measurement to an infinitely squeezed state. In phase space the projection of the second mode of a bipartite state is given by the map [37],

$$\gamma_a^{out} = \gamma_a - C_{ab}(X\gamma_b X)^{MP} C_{ab}^T \qquad d_a^{out} = C_{ab}(X\gamma_b X)^{MP}(m - d_b) + d_a, \tag{2.17}$$

where $X = \text{diag}(1,0,1,0)$, $m = (X_1, 0)$ with X_1 being the homodyne measurement outcome and MP denotes the inverse on the range. The projection from the measurement of the $\hat{p}$ quadrature can be found by using $X = \text{diag}(0,1,0,1)$ and $m = (0, X_1)$. A homodyne is a destructive measurement so the original mode is traced out of the bipartite state.

Heterodyne detection

A homodyne detector can only measure one quadrature at a time. At the cost of 3dB loss two homodyne detectors can be combined using a 50/50 beam splitter to split the signal and measure both quadratures simultaneously as illustrated in Fig. 2.3. In phase space the projection is given by the map,

$$\gamma_a^{out} = \gamma_a - C_{ab}(\gamma_b + \mathbb{I})^{-1} C_{ab}^T, \qquad d_a^{out} = \sqrt{2} C_{ab}(\gamma_b + \mathbb{I})^{-1}(m - d_b^{in}) + d_b^{in}) + d_a^{in}. \tag{2.18}$$

where $m = (x_1, p_1)$ is the vector of the results from a heterodyne measurement on mode $\hat{b}$

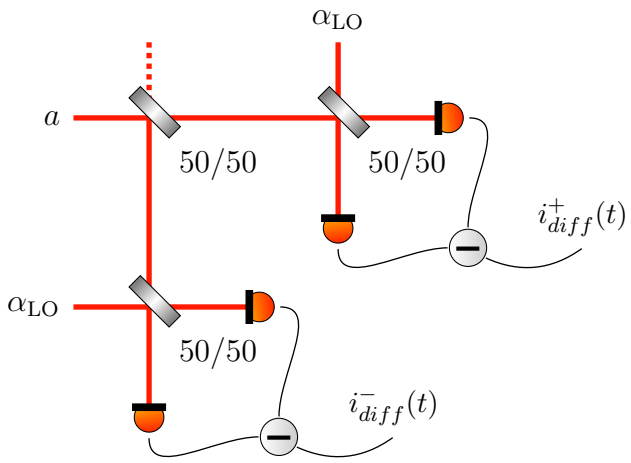


Figure 2.3: A heterodyne detector also know as a dual homodyne. The signal field is split on a 50/50 beam splitter and the resulting beams sent to homodyne detectors which are measuring orthogonal quadratures.

2.2 Optical resonators

Optical resonators are used in this thesis to either define spatial and frequency modes by filtering an incident field or to increase non-linear effects through the resonance of the internal optical field. The most general optical resonators is a Fabry Pérot cavity. This cavity, illustrated in Fig. 2.4, consists of two mirrors, an input coupler (IC) and output coupler (OC), facing each other at some distance L. An optical field inside the cavity will reflect between the two mirrors with resonant modes constructively interfering. The resonant modes of the cavity have a wavelength that is a multiple of the cavity length. For a Fabry Pérot cavity this create standing waves in the cavity that constructively interfere with non-resonant wavelengths destructively interfering. Only the resonant modes will be transmitted through a cavity with the remaining modes reflected off the coupling mirrors. A cavity can be used to select specific frequency and spatial modes from an incident field by clever design of the geometry [38–40]. These properties allow a cavity to be used to filter the spatial and frequency modes from a laser.

As a closed system the internal field annihilation operator, $\hat{a}$, will evolve in time according to Heisenberg's equation of motion,

$$\dot{\tilde{a}} = \frac{1}{i\hbar}[\tilde{a}, H_{\mathrm{rev}}] \tag{2.19}$$

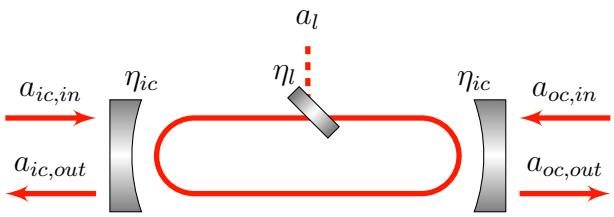


Figure 2.4: A model of an optical resonator with the field $a_{\mathrm{ic,in}}$ coupled through the IC with transmission η_{ic} and the counter propagating field $a_{\mathrm{oc,in}}$ coupled through the OC with transmission η_{oc}. The cavity loss is modelled as a beam splitter with transmission η_{l} which couples the internal field to the environment.

In a closed system the Hamiltonian, H_{rev} is reversible. Open systems have non reversible evolutions through lossy interactions with the surrounding environment. To account for the irreversible interactions extra terms can be added to Eq. (2.19) [41]. The modified equation of motion is know as the quantum Langevin equation and is given by,

$$\dot{\tilde{a}}(t) = \frac{1}{i\hbar}[\tilde{a}, H_{\mathrm{rev}}] - [\tilde{a}, \tilde{c}^{\dagger}](\gamma\tilde{c} + \sqrt{2\gamma}\tilde{b}_{\mathrm{in}}) - (\gamma\tilde{c}^{\dagger} + \sqrt{2\gamma}\tilde{b}^{\dagger}_{\mathrm{in}})[\tilde{a}, \tilde{c}]. \tag{2.20}$$

Here the operator $\tilde{c}$ is the system operator, $\tilde{a}$, coupled to the environment $\tilde{b}$ and γ is the cavity decay. For a lossless passive resonator the Hamiltonian is given by Eq. (1.29) where $\omega = \Omega$ is a resonant frequency. Using Eq. (1.29) with Eq. (2.20) gives the following equations of motion for an optical cavity coupled to the environment [21],

$$\dot{\tilde{a}}(t) = -(\gamma + i\Delta)\tilde{a} + \sqrt{2\gamma_{ic}}\tilde{a}_{ic,in} + \sqrt{2\gamma_{oc}}\tilde{a}_{oc,in} + \sqrt{2\gamma_{l}}\tilde{a}_{l}. \tag{2.21}$$

Here the cavity decay rate γ is given by $\gamma = \gamma_{\mathrm{ic}} + \gamma_{\mathrm{oc}} + \gamma_{l}$, the cavity detuning between the resonant frequency and the frequency of the input field, Ω', is given by $\Delta = \Omega - \Omega'$ and the decay rates due to the IC, OC and loss are given by,

$$\gamma_{\mathrm{ic}} = \eta_{\mathrm{ic}}/2\tau, \tag{2.22}$$

$$\gamma_{\mathrm{oc}} = \eta_{\mathrm{oc}}/2\tau, \tag{2.23}$$

$$\gamma_{\mathrm{l}} = \eta_{\mathrm{l}}/2\tau, \tag{2.24}$$

where η is the transmission for the respective coupling mirror and τ is the round trip time. To simplify the equations of motion the field $\tilde{a}$ will be modelled in the rotating reference frame of the incident field and the detuning will be set to $\Delta = 0$. A solution for Eq. (2.21) can be found using the Fourier transform property $\mathbb{F}(\dot{a}(t)) = i\omega\mathbb{F}(g(t))$ to give,

$$\hat{a} = \frac{-1}{\gamma + i\omega}\left(\sqrt{2\gamma_{ic}}\hat{a}_{ic,in} + \sqrt{2\gamma_{oc}}\hat{a}_{oc,in} + \sqrt{2\gamma_{l}}\hat{a}_{l}\right). \tag{2.25}$$

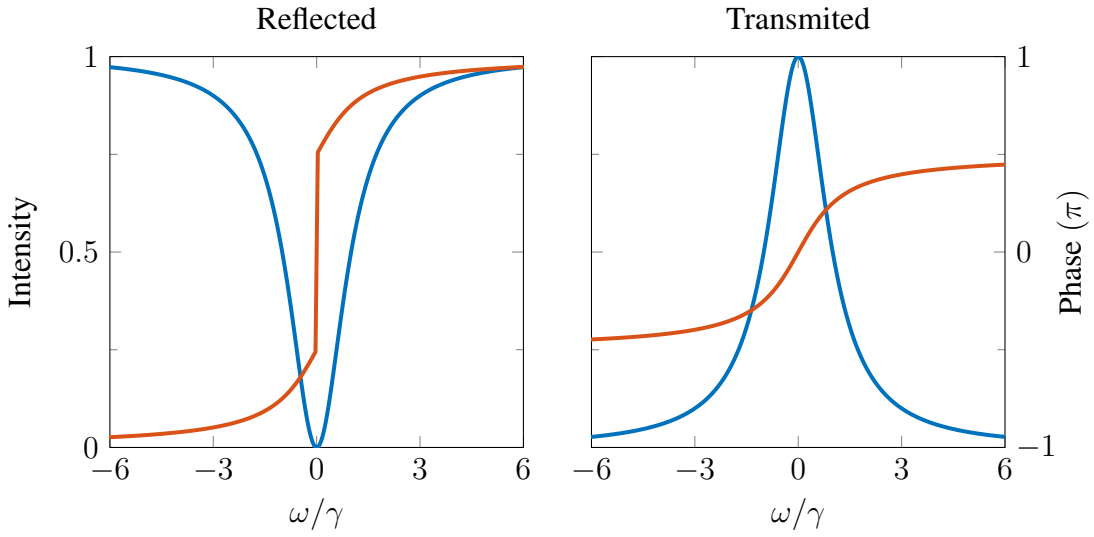


Figure 2.5: The intensity normalized to the power of $a_{\mathrm{ic,in}}$ (blue) and phase (red) of the reflected, $a_{\mathrm{ic,out}}$, and transmitted, $a_{\mathrm{oc,out}}$, fields using the classical analysis of the cavity fields. The cavity parameters used here are from the cavity discussed in Sec. 3.2.2. The fields $a_{\mathrm{oc,in}}$ and a_l taken to be vacuum modes. The discontinuity in the phase of the reflected field is caused by the reflected field disappearing when the cavity is on resonance.

The output fields $a_{ic,out}$ and $a_{oc,out}$ in the Fourier domain can be found by using the boundary conditions,

$$\hat{a}_{m,\mathrm{out}} = \sqrt{2\gamma_m}\hat{a} + \hat{a}_{m,\mathrm{in}}, \tag{2.26}$$

to give,

$$\hat{a}_{m,\mathrm{out}} = \frac{(\gamma + i\omega - 2\gamma_m)\hat{a}_{m,\mathrm{in}} - 2\sqrt{\gamma_m\gamma_n}\hat{a}_{n,\mathrm{in}} - 2\sqrt{\gamma_m\gamma_l}\hat{a}_l}{\gamma + i\omega}. \tag{2.27}$$

Here $m, n = \{\mathrm{ic}, \mathrm{oc}\}$. The classical analysis of a cavity can be made using the linearisation of operators in Eq. (2.27) and ignoring the fluctuating terms. Setting $\alpha_{\mathrm{oc,in}} = \alpha_l = 0$ gives the transfer functions from the input field $a_{\mathrm{ic,in}}$ to the reflected, $a_{\mathrm{ic,out}}$, and transmitted $a_{\mathrm{oc,out}}$ fields,

$$\frac{\alpha_{\mathrm{ic,out}}}{\alpha_{\mathrm{ic,in}}} = \frac{2\gamma_{\mathrm{ic}} - i\omega - \gamma}{i\omega + \gamma} \tag{2.28}$$

$$\frac{\alpha_{\mathrm{oc,out}}}{\alpha_{\mathrm{ic,in}}} = \frac{2\sqrt{\gamma_{\mathrm{ic}}\gamma_{\mathrm{oc}}}}{i\omega + \gamma} \tag{2.29}$$

When $\omega \approx 0$ the cavity will have maximum transmission of the input fields, $a_{\mathrm{ic,in}}$ and $a_{\mathrm{oc,in}}$, through the cavity. On the other hand when $\omega \gg \gamma$ the cavity will reflect all of the input fields e.g. $\hat{a}_{\mathrm{m,out}} = \hat{a}_{\mathrm{m,in}}$. The 3 dB point of a cavity is given where $\omega = \gamma$. This leads to a nice result where the spectrum of an input field, $\hat{a}_{\mathrm{ic,in}}$, can be filtered to the shot

Figure 2.6: Second order non-linear process. Down conversion, (a), takes a single photon of frequency 2Ω and produces two photons of frequency Ω. Up conversion, (b), takes two photons of frequency Ω and converts them to a signal photon at frequency 2Ω.

noise limit when $\omega \gg \gamma$ and the other inputs are vacuum modes.

2.3 Second order optical non-linearity

When an optical field is passed through a dielectric medium an atomic polarisation, P, is induced on the dipole moments of the medium. With light far detuned from the resonance of the medium the electromagnetic field create a macro-scopic atomic polarisation oscillating at the frequency of the field. These oscillations can be re-emitted back into the optical field. In a non-linear medium these oscillations can occur at harmonic frequencies of the original field. The polarisation of the resulting optical field can be written as the series [21],

$$P = \epsilon_0 \left(\chi E + \chi^{(2)} E^2 + \chi^{(3)} E^3 + \dots \right), \tag{2.30}$$

where χ is the linear susceptibility and $\chi^{(i)}$ is the ith non-linear susceptibility of the medium. The second order non-linearity, of interest in this thesis, are used to either generate a second harmonic or squeeze a quadrature of the fundamental field. This thesis will limit the description of optical non-linearity to degenerate parametric down conversion. This is a simple case of non linearity where a single photon in a pump field, b, of frequency 2Ω splits into two photons of the fundamental field, a, of frequency Ω in some non-linear material. The non-linearity of the material is parameterised by the second-order non-linear susceptibility, $\chi^{(2)}$.

Phase matching condition

As with any system both energy and momentum must be conserved. In a degenerate second order non linear process the energy conservation is satisfied by $\Omega_2 = \Omega_1 + \Omega_1'$ and momentum is satisfied by the wave vectors $\boldsymbol{k}_2 = \boldsymbol{k}_1 + \boldsymbol{k}_1'$. Here ' is used to represent the pump field. If the fundamental and pump are co-propagating through the nonlinear medium then the non-linear interaction is maximised if both propagate with the same

phase. Normally a material does not satisfy this condition as the refractive index increases with frequency. To match the propagation of the fundamental and pump this thesis uses a method called quasi-phase matching. For this method the domains of the material are periodically poled to invert the crystal axis. This changes the sign of the non-linear susceptibility and reverses the accumulation phase difference between the two fields. That is the fundamental and second harmonic are re-phased every poling period which is ideally once the waves are $\pi/2$ out of phase [42]. To perfectly match their propagation the material can be heated or cooled. A more complete description of this and other methods used to match the phase can be found in [42].

2.3.1 Optical parametric amplification

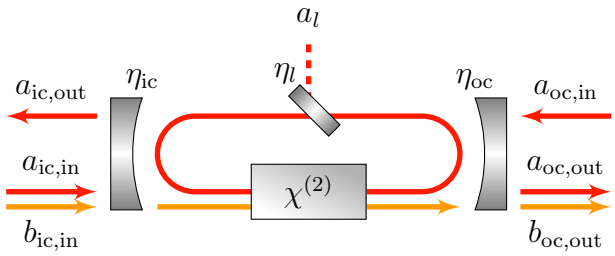


Figure 2.7: A cavity with a non-linear crystal. The pump field $b_{\mathrm{ic,in}}$ is passed through the IC and makes a single pass through the non-linear crystal.

The non-linear process can be enhanced by placing the medium in an optical cavity as illustrated in Fig. 2.7. In a closed system the Hamiltonian that describes an Optical Parametric Amplifier (OPA) is given by

$$H_{\chi^{(2)}} = \hbar\Omega\hat{a}^\dagger\hat{a} + 2\hbar\Omega\hat{b}^\dagger\hat{b} + i\hbar\frac{\Lambda}{2}\left(\hat{a}^{\dagger 2}\hat{b} - \hat{a}^2\hat{b}^\dagger\right). \tag{2.31}$$

Here the first two terms represent the energy in the pump, b, and fundamental, a with Ω being the angular frequency of the fundamental. The third term describes their interaction. The interaction strength is parameterised by Λ which is a function of $\chi^{(2)}$ and other experimental parameters including phase matching and beam focusing.

Using the quantum Langevin equation, Eq. (2.20), with the Hamiltonian, Eq. (2.31), the equations of motion for a cavity with second order non-linearity are found to be [43],

$$\dot{\tilde{a}} = -\gamma_a\tilde{a} + \Lambda\tilde{a}^\dagger\tilde{b} + \sqrt{2\gamma_{ic,a}}\tilde{a}_{ic,in} + \sqrt{2\gamma_{oc,a}}\tilde{a}_{oc,in} + \sqrt{2\gamma_{l,a}}\tilde{a}_l, \tag{2.32}$$

$$\dot{\tilde{b}} = -\gamma_b\tilde{b} - \frac{\Lambda}{2}\tilde{a}^2 + \sqrt{2\gamma_{ic,b}}\tilde{b}_{ic,in} + \sqrt{2\gamma_{oc,b}}\tilde{b}_{oc,in} + \sqrt{2\gamma_{l,b}}\tilde{b}_l. \tag{2.33}$$

Here γ_a is the cavity decay rate for the fundamental field and $gamma_b$ the decay rate for the pump. This thesis will only consider singly resonant OPAs. This allows the simplification of $\gamma_{oc,b} = \gamma_{l,b} = 0$ by assuming the pump does not couple to the environment. The pump can also be assumed to have an evolution rate much slower than the fundamental to give $\dot{\tilde{b}} = 0$. To produce squeezing, each of the OPAs found in this thesis are operated below threshold yielding approximately no pump depletion. With these assumptions the equation of motion of the internal pump field of the cavity becomes,

$$\tilde{b} = -\sqrt{\frac{2}{\gamma_b}}\tilde{b}_{\mathrm{ic,in}}, \tag{2.34}$$

and the equation of motion for the fundamental field simplifies to,

$$\dot{\tilde{a}} = -\gamma_a\tilde{a} + \sqrt{\frac{2}{\gamma_b}}\Lambda\tilde{a}^{\dagger}\tilde{b}_{\mathrm{ic,in}} - \sqrt{2\gamma_{ic,a}}\tilde{a}_{\mathrm{ic,in}} - \sqrt{2\gamma_{oc,a}}\tilde{a}_{\mathrm{oc,in}} - \sqrt{2\gamma_{l,a}}\tilde{a}_l. \tag{2.35}$$

Classical description of an OPA

A classical description of an OPA can be made in the same way it was for the linear resonator by only considering the real coherent component of the linearised operators in Eq. (2.35). Taking $\alpha_l = \alpha_{oc,in} = 0$ and the OPA as being in steady state gives the solution,

$$\alpha = \frac{2\gamma_{ic,a}(1 + g/\gamma_a)}{\gamma_a(1 - |g|^2/\gamma_a^2)}\alpha_{ic,in}, \tag{2.36}$$

where the non-linear gain, g, is given by,

$$g = \Lambda\sqrt{\frac{2}{\gamma_b}}\beta_{ic,in}e^{i\phi}. \tag{2.37}$$

Here ϕ is the phase between the pump and the fundamental fields. The classical gain from an OPA, g_r, can be found using the output relation Eq. (2.26) to compare the power of the amplified transmitted field with the unamplified field. This gives,

$$g_r = \frac{P^{\mathrm{a}}_{\mathrm{oc,out}}(g)}{P^{\mathrm{a}}_{\mathrm{oc,out}}(0)} = \frac{(1 + g/\gamma_a)^2}{(1 - |g|^2/\gamma_a^2)^2} \tag{2.38}$$

This is known as the regenerative gain of the OPA [40]. As the gain, g, increases the more pump power is transferred into the fundamental and g_r increases. Once the pump power reaches threshold of the optical parameteric oscillator (OPO), $|g| > \gamma_a$, the regenerative gain will go to infinity and the cavity will start to self oscillate causing the squeezing

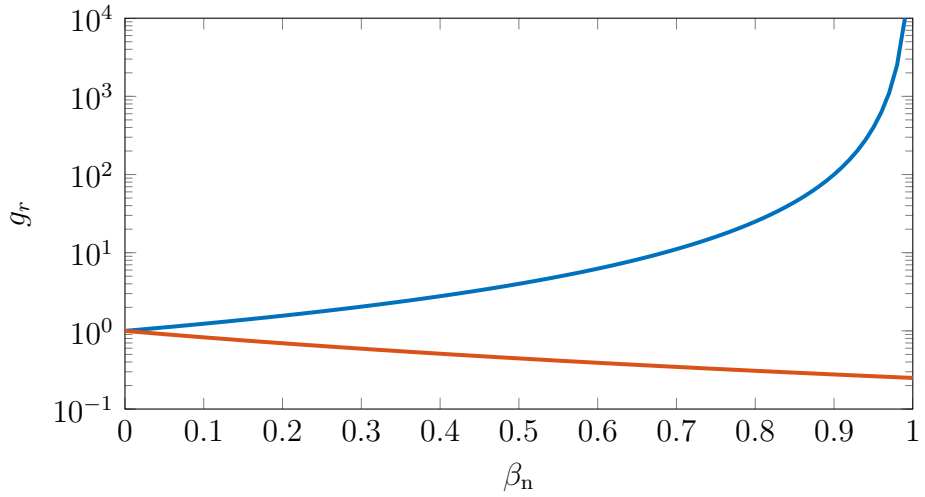


Figure 2.8: Regenerative gain for a OPA cavity vs. the normalised pump parameter for $\phi = 0$ (blue) and $\phi = 90$ (red).

spectrum to split [19]. The threshold of the pump is given by,

$$\beta_{\mathrm{th}} = \frac{\gamma_{\mathrm{a}}\sqrt{\gamma_{\mathrm{b}}}}{\Lambda\sqrt{2}} \tag{2.39}$$

The equations of motion can be related to the pump threshold through the normalised pump parameter,

$$\beta_{\mathrm{n}} = \frac{g}{\gamma_{\mathrm{a}}} = \frac{\beta_{\mathrm{ic,in}}}{\beta_{\mathrm{th}}} \tag{2.40}$$

Semi-classical description

A semi-classical description of the squeezing spectrum of the output field can be made by now considering the fluctuating terms in the linearised operators and substituting Eq. (2.37) in Eq. (2.35) to get,

$$\dot{\tilde{a}} = -\gamma_a a + g\tilde{a}^\dagger - \sqrt{2\gamma_{ic,a}}\tilde{a}_{ic,in} - \sqrt{2\gamma_{oc,a}}\tilde{a}_{oc,in} - \sqrt{2\gamma_{l,a}}\tilde{a}_l \tag{2.41}$$

Then using the definition $\dot{x} = \dot{a} + \dot{a}^\dagger$ and $\dot{p} = i(\dot{a}^\dagger - \dot{a})$ with the boundary condition Eq. (2.26) the equation of the transmitted field in the frequency domain are found to be,

$$\hat{x} = \frac{(wi + \gamma_a + g + 2\gamma_{oc})\hat{x}_{oc,in} + 2\sqrt{\gamma_{ic}\gamma_{oc}}\hat{x}_{ic,in} + \sqrt{\gamma_l\gamma_{oc}}\hat{x}_{l,in}}{wi - g + \gamma_a} \tag{2.42}$$

$$\hat{p} = \frac{(wi + \gamma_a - g + 2\gamma_{oc})\hat{p}_{oc,in} + 2\sqrt{\gamma_{ic}\gamma_{oc}}\hat{p}_{ic,in} + \sqrt{\gamma_l\gamma_{oc}}\hat{p}_{l,in}}{wi + g + \gamma_a} \tag{2.43}$$

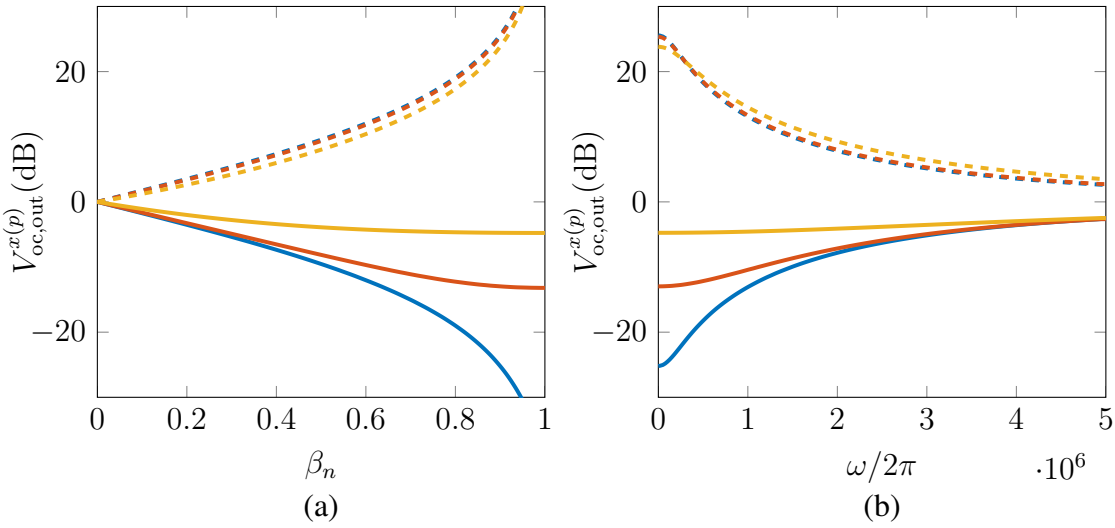


Figure 2.9: Demonstration of the effect of normalized pump power on squeezing and anti-squeezing (dashed) with $\omega = 0$, (a), and cavity loss on the squeezed and anti-squeezed spectrum, (b). The cavity modelled here uses the parameters, $\eta_{\mathrm{ic}} = 0.999975$, $\eta_{\mathrm{oc}} = 0.8$, $L = 0.45m$. The cavity loss, η_{l} is set to 0 (blue), 0.005 (red), and 0.05 (yellow). The escape efficiency for these losses are 0.9998, 0.95 and 0.67. For plot (b) $x = 0.9$.

Finding the variance of these two operators gives with the assumption that all of the input fields are vacuum states i.e $V^a_{ic,in} = V^a_{oc,in} = V^a_{l,in} = 1$,

$$V^{x(p)}_{\mathrm{oc,out}} = 1 + (-)\frac{\gamma_{oc}}{\gamma_a}\frac{4(g/\gamma_a)}{(\omega/\gamma_a)^2 + (1 + (-)g/\gamma_a)^2}. \tag{2.44}$$

From this equation the escape efficiency is defined as $\eta_{\mathrm{esc}} = \gamma_{\mathrm{oc}}/\gamma_a$. The variance can be also be written in terms of the normalised pump parameter to give,

$$V^{x(p)}_{\mathrm{oc,out}} = 1 + (-)\eta_{\mathrm{esc}}\frac{4\beta_{\mathrm{n}}}{(\omega/\gamma_a)^2 + (1 + (-)\beta_{\mathrm{n}})^2} \tag{2.45}$$

To generate squeezing with an OPA there is a trade off between increasing η_{esc}, while at the same time keeping γ_a at a reasonable level. Increasing γ_a will increase the threshold power making it harder to provide enough power to pump the crystal near threshold. If η_{esc} is too small then the magnitude of the state is decreased. The effect of varying these parameters is shown in Fig. 2.9. Decreasing the escape efficiency reduces the squeezing at lower frequencies and has little effect on the amount of anti-squeezing. Increasing the pump power increases the amount of squeezing and anti-squeezing exponentially near the threshold power.

2.4 Feedback control

Throughout this thesis there are multiple occurrences where feedback control has been used to keep a cavity on resonance or keep two fields in quadrature or phase. There are a number of methods that can be used for feedback control. This section will provide a brief summary of methods used in this thesis. Consider the general feedback loop in Fig. 2.10 where a "plant" has an output y. A "measurement", y_m, is made on the output. The measurement of the output is then used by a "controller" to control the state of the plant to a reference level r. For this thesis the reference r is always set to 0 making $y_m = e$. This section is split into two sections to address how the error signal, e, is generated and describe the controllers used.

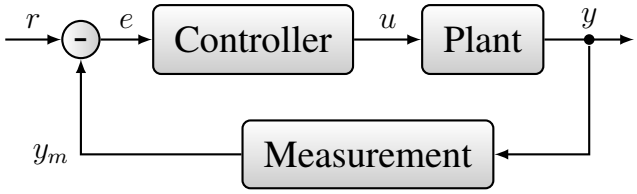


Figure 2.10: Typical feedback loop

2.4.1 Measurement

The PDH method

The PDH method of generating an error signal for a cavity is very common in optics. This technique uses the beating between the carrier and a sideband modulation [44]. The general setup for this method is shown in Fig. 2.12 along side an example error signal. For a generic cavity the reflected signal from the IC will change phase and intensity as the incident field detunes from the cavity resonance. This is represented in the phasor diagram illustrated in Fig. 2.11(a) where the phasor for the reflected field rotates around a circle. The case where the incident field has a modulation $\omega_m \gg \gamma$ is shown in Fig. 2.11(b). The modulations will beat together to create a signal oscillating at $2\omega_m$. When the cavity is near resonance the carrier will create an asymmetry in the beating sidebands that oscillates at ω_m. This asymmetry will create the PDH error signal and can recovered by demodulating the detected signal in quadrature. The remaining terms after demodulation are filtered out with a low pass filter. The recovered error signal is given by,

$$e = -2\sqrt{P_c P_s}\mathrm{Im}\{F(w)F^*(w+\omega_m) - F^*(w)F(w-\omega_m)\}, \tag{2.46}$$

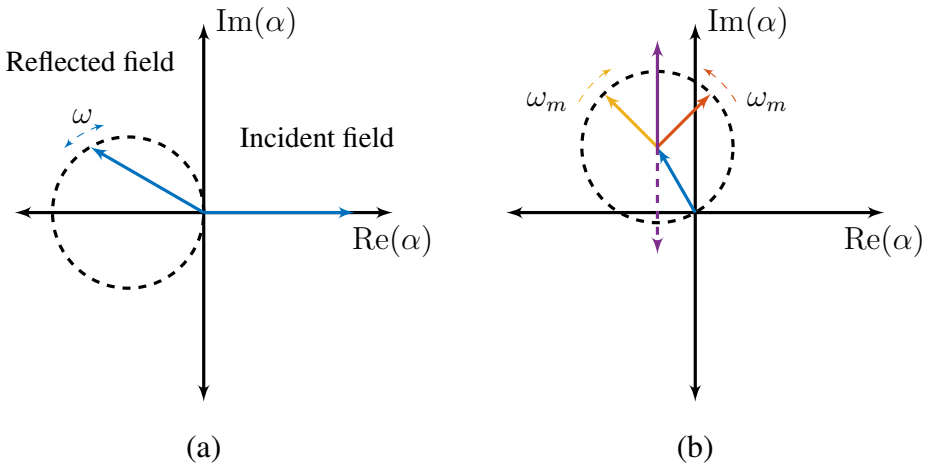


Figure 2.11: A phasor plot showing the phase of the reflected incident field without (a) and with (b) sideband modulations. The phasor of the reflected field from a critically coupled cavity will rotate around a circle as the cavity is detuned from resonance. Adding sideband modulation to the incident field creates beating in the detected signal. The two sidebands (yellow and red) will beat together to create a beating signal (purple) at 2ω which will vary at ω when the incident field is close to resonance.

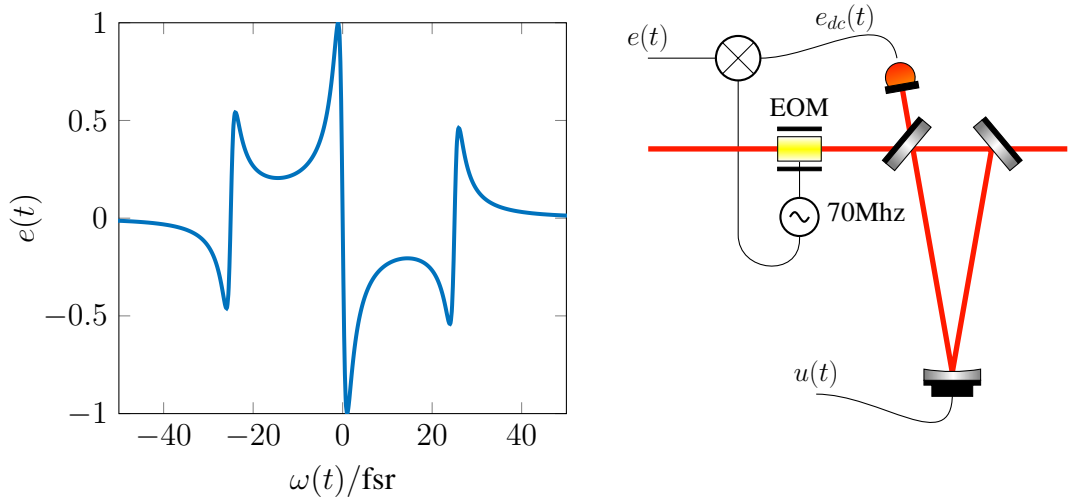
where P_c and P_s are the power in the carrier and modulation respectively and $F(\omega)$ is the transfer function of the reflected signal in the Fourier domain given in Eq. (2.28).

The in phase ω_m signal is generally discarded but can be used to lock the phase of the pump to the fundamental in an OPA cavity. For this the modulation needs to be within the linewidth of the cavity. This will change the phase at which the reflected signal will need to be demodulated to recover the PDH error signal. With a pumped OPA the internal cavity field will detune and create imbalance between the lower and upper sidebands. Imbalance will create an error signal orthogonal in the detected signal to the PDH error signal. To find the angle of demodulation for this locking method the PDH error signal needs to be demodulated at an angle that makes it independent of the pump phase. The error signal for the pump is recovered from the orthogonal demodulation from the PDH error signal [45].

Difference detection

Difference detection is the easiest method considered here to generate an error signal. With two coherent beams mixed on a 50/50 beam splitter the detected signals are subtracted to create the error signal,

$$i(t) = g_{\mathrm{D}} \left(\frac{1}{2}\alpha_1(t) + \frac{1}{2}\alpha_2(t) + \alpha_1(t)\alpha_2(t)\cos\theta \right) \tag{2.47}$$



(a) (b)

Figure 2.12: An example of the typical use of PDH locking in this thesis. The example cavity is discussed in Sec. 3.2.2. The modulation is set to $25 \times \gamma$. The input $u(t)$ is used to control the cavity. The plot of $e(t)$ is found by scanning $u(t)$ with a ramp function.

Subtracting the detected signal from both output ports will give the following error signal

$$i(t)_3 - i(t)_4 = 2g_{\mathrm{D}}\alpha_1(t)\alpha_2(t)\cos\theta \tag{2.48}$$

This gives a simple cosine error signal with the important linear section and zero crossing around $\pi/2$ allowing the input beams to be easily locked in quadrature. Importantly the zero crossing of this error signal is independent of the power of the input beams.

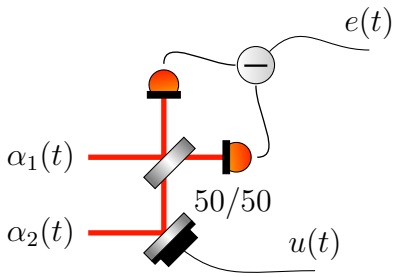


Figure 2.13: Difference detection. Two optical fields, $\alpha_1(t)$ and $\alpha_2(t)$ are interfered on a 50/50 beam splitter. The signal $u(t)$ controls the phase between the two fields with a piezo driven mirror. The output ports are detected and subtracted to create $e(t)$.

2.4.2 Controllers

State-Machine Controller

This controller, developed by a former member of the group, Seiji Armstrong [46, 47], was used to perform almost all the locking for this thesis. This controller uses the state-machine logic illustrated in Fig. 2.14. In the default state, Scan, the controller will scan the plant with a low frequency ramp function. When the user inputs a lock command the scan will continue until the plant output drops below a threshold value, e_t. The controller will transition to the lock state and engage a PI controller in a feedback loop. If the output ever increases above e_t the controller will scan the cavity back to the locking point. For a cavity the signal e_{dc} is used to determine if the plant is above or below the threshold. If the user inputs a hold command the output of the controller is held at a constant value. The controller is implemented in LabView and runs on a National Instruments FPGA with both analogue inputs and outputs.

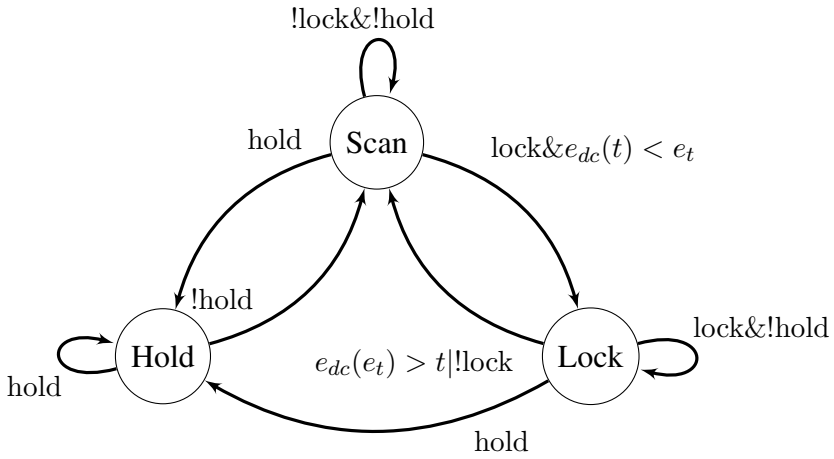


Figure 2.14: State machine PDH controller. Hold, lock and e_t are set by the user. $e_{dc}(t)$ for a PDH lock is the error signal before the mixer. For difference detection $e(t) = e_{dc}(t)$

Microcontroller locking

A scheme using a microcontroller was proposed in Ref. [48, 49]. This method employs the simple algorithm illustrated as a flowchart in Fig. 2.15. The original implementation is designed to run on a microcontroller however for this thesis it was implemented using an FPGA. This algorithm is easy to implement and tune.

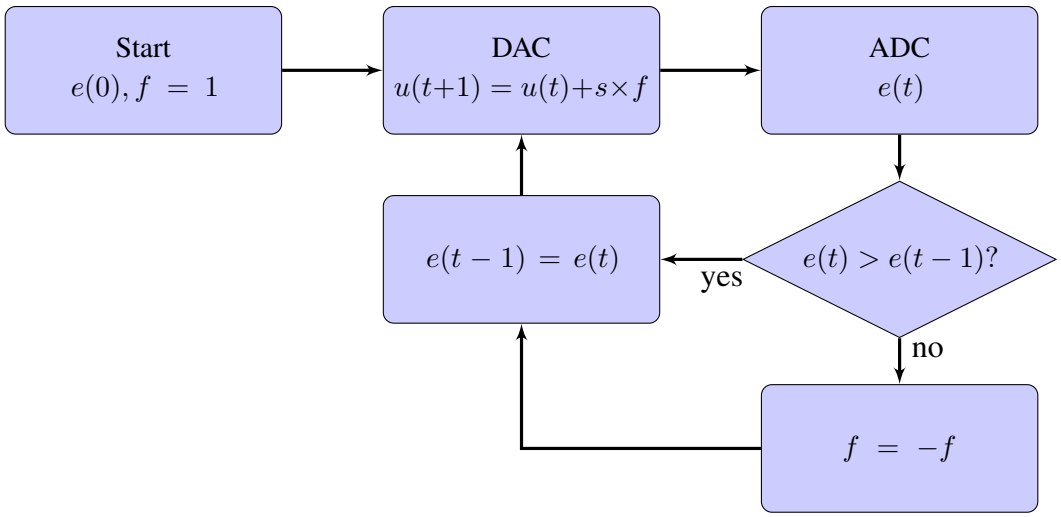


Figure 2.15: Microcontroller locking method flow chart. This algorithm updates the output by stepping the DAC output by s. If the error signal starts increasing the algorithm will change the sign of s using f.

Chapter 3

Squeezed State Generation at 1550nm

3.1 Introduction

This chapter details the work to generate highly squeezed states. The purpose of the squeezed states is to use them in demonstrations of quantum control, estimation and communication protocols. Squeezed states are a major resource for the CV community. In this thesis they are primarily used in the context of QKD but they have other applications in in broader communications protocols [50, 51], increasing the precision of phase estimation [52] and lowering the noise in the detection of gravitational waves [53, 54] to name a few. As well as this they are also used to create a variety of other non Gaussian states [27] for numerous other protocols and applications. A wider summary of these applications can be found in Ref. [55]. There are a number of different methods for generating squeezed states though this chapter will only discuss squeezed states generated from an OPA. The highest recorded squeezing has been 15dB achieved with a semi-monolithic cavity [56]. Another OPA cavity design commonly used and the one found in this chapter is the bow-tie cavity [57, 58]. Unlike the standing wave semi-monolithic cavity the bow tie cavity generates a travelling wave and can be made to be less prone to anti-squeezing coupling into the squeezed quadrature through back reflections with a trade off of greater intra-cavity losses. These losses are a result of the larger number of optical components used in a bow-tie cavity. This chapter will present the results of the development of a low intra-cavity loss OPA cavity. The OPA has so far achieved an 11 dB squeezed vacuum state with an intra-cavity loss of 0.3% using periodically poled Potassium Titanyl Phosphate (ppKTP) as the non-linear crystal.

No publication has come from this work as yet. This chapter is a summary of the current results. Much of the detailed design decisions for the components around the OPA have been omitted. This chapter is divided into two main sections. The first Sec. 3.2 will detail the squeezing experiment including a brief description of the parameters of each major component. The results of the experiment are presented in Sec. 3.3 and a discussion on the planned use for the squeezed states is given in Sec. 3.4.

3.2 Experiment

An overview of the experiment is given in the schematic found in Fig. 3.1. The laser used for this experiment is first split into two paths. One is to provide the OPA cavity locking signal and local oscillator. The other is used in an SHG cavity to generate a 775 nm beam for the pump. The first beam path is passed through a mode cleaning cavity (MCC) before being split again to a LO path and the locking beam for the OPA. The details for each of the major components in Fig. 3.1 are given in the subsequent chapters.

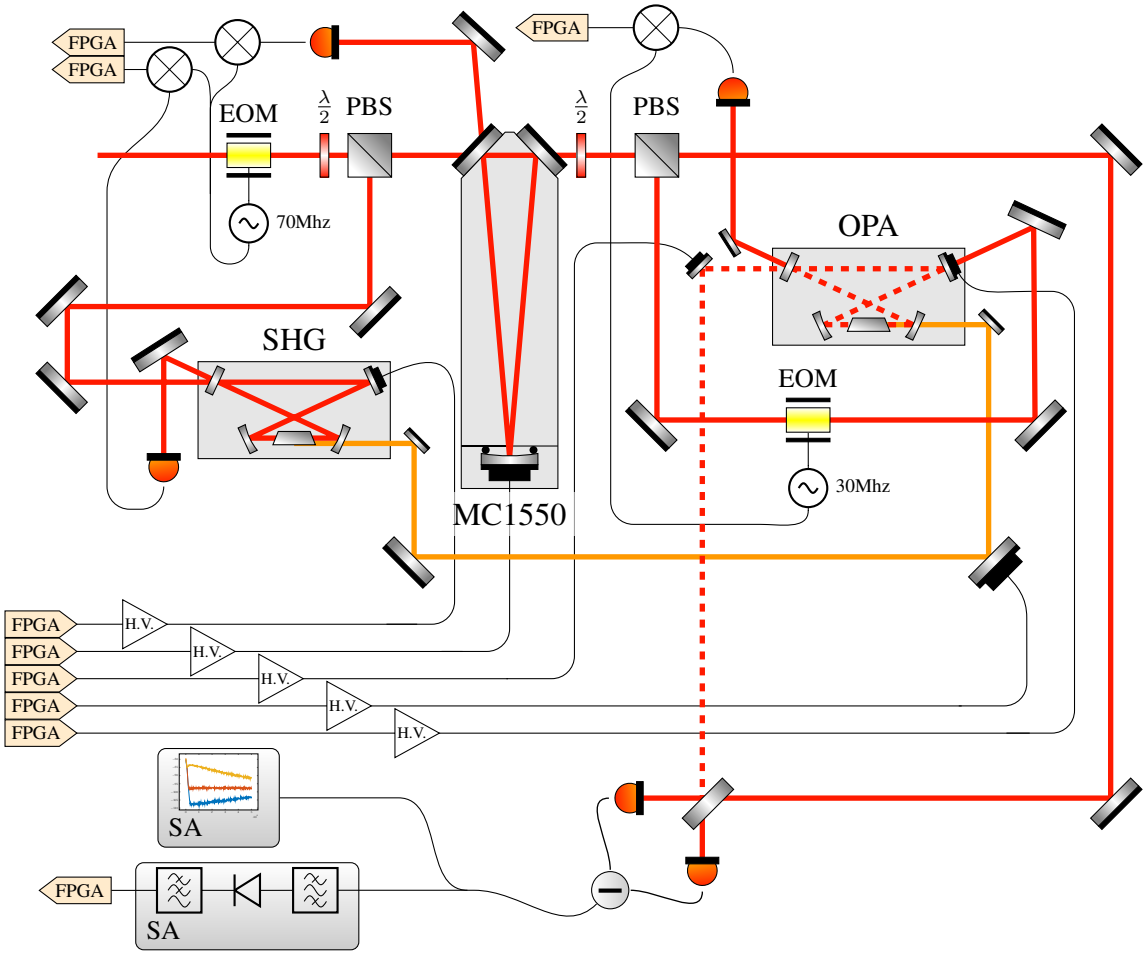
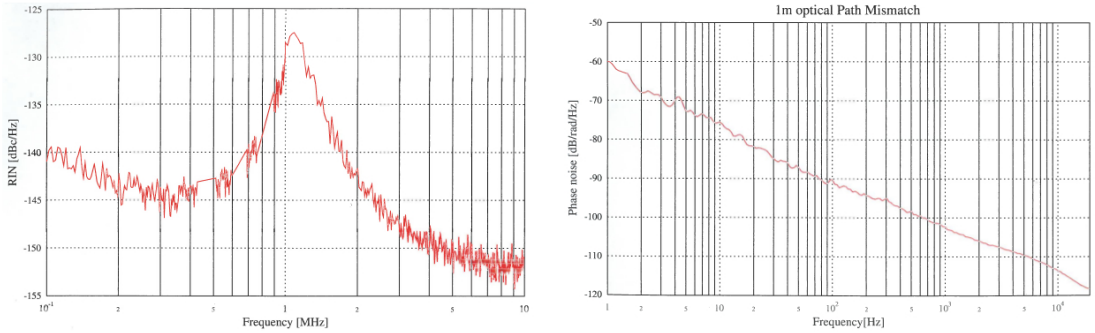


Figure 3.1: Schematic of the experiment to generate squeezed states using 1550nm. The laser produced by 1550nm fiber laser source (Sec. 3.2.1) is split into three paths. The first path is used in an SHG cavity (Sec. 3.2.3) to generate 775nm light for the pump. The second path is used to lock the OPA cavity (Sec. 3.2.4) length and the third path is used as the LO for the homodyne detector (Sec. 3.2.5). A MCC (Sec. 3.2.2) is used to clean the spatial and frequency modes of the LO and the locking beam for the OPA. Each cavity and path length is locked using feedback with an FPGA controlling the cavity lengths (Sec. 3.2.6).

3.2.1 The Laser

For this work a NKT Photonics Koheras BoostiK single frequency fibre laser system was chosen based on its use in other labs and the poor reputation of similar lasers. The seed laser for the system is an AdjustiK C15 shot noise limited co-doped eribium/ytterbium fiber laser based on the Basik C15. From the Koheras range this laser has the lowest relative intensity noise (RIN). This low RIN comes at the cost of increased phase noise in comparison to other AdjustiK lasers [59]. The seed laser is amplified to provide power up to 5W. The line width of the laser system is reported to be 8kHz with a RIN peak at 1.1MHz.



(a) (b)

Figure 3.2: RIN (a) and Phase noise (b) plots obtained from the laser test report [60]

3.2.2 Mode Cleaning Cavity

The MCC is the first element on the beam path providing the seed and local oscillator. The role of a MCC is to reduce spectral noise and clean the spatial mode of the beam. The design of this cavity is based on the previous experiments conducted at 1064nm by the group [40, 61].

The MCC is a three mirror ring cavity as shown in Fig. 3.1 with a designed path length of 800 mm. Each mirror is mounted on to a cylinder of Invar, chosen for its low thermal expansion. The beam path through the Invar cylinder is machined out. The input and output couplers are planar mirrors with reflectivity of 99.5% mounted with an angle of incidence of $43.5°$. The length of the cavity is controlled by a Piezo pushing on the highly reflective back mirror. The back mirror and the Piezo are pressed into a rubber o-ring by the end cap of the cavity. The Piezo and mirror are pre-loaded with a force of roughly 3kN. By pre-loading the Piezo the resonant frequency of the Piezo-mirror system increases [21] allowing for larger locking bandwidths. The radius of curvature of the back mirror is 1 m giving a cavity waist of around 0.63 mm at a wavelength of 1550nm.

The finesse of this cavity was calculated to be 620. As the laser is fiber based and already has a low intensity noise outside the line width of the cavity to begin with this cavity has very little effect on the output beam frequency modes. However, it provides a near perfect spatial Gaussian mode which is a necessary requirement to achieve high homodyne detection efficiency.

3.2.3 Design of the OPA and SHG Cavities

Both the SHG and OPA cavities were designed to be identical to make mode matching easier. The design is a bowtie singly resonant cavity at 1550nm with a non-linear crystal at the waste. The mechanical design is shown in Fig. 3.3 and is based on previous squeezers built by the group [34] with a few improvements to the crystal oven design and Piezo mount.

The cavity is built on a base of solid aluminium with optics mounts that are designed to easily adjust the distance between the two concave mirrors. The non-linear crystal is positioned at the waist of the cavity in an oven constructed out of copper and heated by a Peltier device which is contacted to a larger copper heatsink. The oven assembly is glued together. To control the length of the cavity there is a Piezo controlled mirror on one side of the cavity glued to an aluminium block. This block features a taper from the front to the rear in an attempt to reduce mechanical oscillations. The rest of the mirrors were mounted using half inch low drift Polaris kinematic mirror mounts from Thorlabs.

The chosen non-linear crystal was 16mm long ppKTP crystal with a poling period of 24.7 μm from RAICOL crystals. The KTP material was chosen as the nonlinear medium due to its almost perfect transparency at the 1550nm wavelength [62]. The two crystal facets were super-polished to an rms accuracy better than 1 angstrom and coated with a low loss anti-reflection coating at 1550nm to minimise the OPA intracavity losses. The facets were also polished at an angle of 1.15° to minimise back reflection into the cavity mode.

The cavities were designed to be singly resonant so the mirrors used all have a transmission of $> 99.9\%$ at a wavelength of 775nm. The two bottom mirrors and the Piezo driven mirror are highly reflective (HR) with a reflectivity of 99.9975% at 1550 nm. The remaining mirror is used as the IC for the SHG and OC for the OPA and has a reflectivity of 90% at 1550nm. The two bottom mirrors have a radius of curvature of 50 mm and positioned to give a beam waist of approximately 34 μm located inside the non-linear crystal. This beam waist is close to the optimum for the OPA/SHG non-linear interaction as predicted by theory [63].

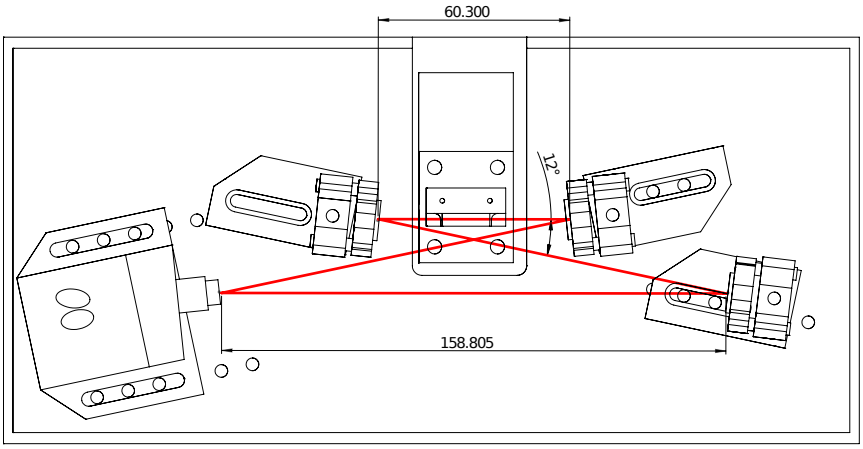


Figure 3.3: Mechanical design of the SHG and OPA cavities. The Piezo and crystal oven assemblies are glued together using vacuum compatible epoxy. The total path length of the cavity is 0.45m

SHG

As shown in Fig. 3.1, the 1550nm light is tapped off for the SHG using a half wave plate and a PBS before the MCC. The input is coupled through the partially reflecting (PR) mirror of the cavity. The upconverted 775nm light is coupled out of the cavity through the first curved mirror and then collimated with a single lens. The efficiency of the SHG was measured to be 71% with 560 mW of 1550 nm light. More details can be found in Ref. [64, 65].

Using the SHG cavity the loss of the non-linear crystal was measured to be 0.3%. This was measured by replacing the IC with a HR mirror and measuring the change in the finesse of the cavity with and without the crystal. The non-linear interaction strength was found to be $\Lambda = 271$ through measurement of an SHG field after a signal pass through the non-linear crystal.

3.2.4 OPA Cavity

For the OPA cavity the design is turned around so the IC is now the Piezo driven HR mirror and opposite PR mirror is used as the OC. Taking the cavity single pass loss of 0.3% the resulting escape efficiency was estimated to be 0.97. The pump is mode matched into the OPA through one of the convex mirrors. The maximum observed regenerative gain was 1440 with 591mW of pump power.

The cavity being seeded through a HR mirror meant that a PDH error signal on reflection had an extremely poor signal-to-noise ration and could not be used to stabilise the cavity length. For this reason the cavity is locked on transmission. From the theory presented in Sec. 2.3.1 the spectrum of the OPA is filtered by the cavity to give the maximum

squeezing at the DC band. For this OPA the linewidth is 10.9Mhz. Since the squeezed state would be contaminated at low frequencies with the laser noise with a seed beam the cavity was locked with a counter-propagating field. This meant that the OPA generated a vacuum squeezed state which presented an interesting control problem for locking the pump phase and homodyne quadrature.

3.2.5 Homodyne detector

The homodyne detector used achieves a dark noise clearance of 18dB below the shot noise. The phase between the electronic signals from the two detectors in the homodyne was tuned to give a 40dB common mode rejection from the local oscillator. The detectors used high efficiency ($> 99\%$) InGaAs p-i-n diodes. To reduce losses on the squeezed light beam path all of the mode matching for the homodyne detector was done on the LO beam path to give a fringe visibility[1] between the modes of $> 99.5\%$.

3.2.6 Cavity and path length locking

The cavity length locking for this experiment was done using the PDH method with a modified version of the controller discussed in Sec. 2.4.2 [46]. The modifications to the controllers code made the locks more reliable to acquire lock for a cavity. See App. B for details of the modification. A new HV amp was also developed for this experiment to take advantage of the lower voltage Piezo devices with the details given in App. A.2.

For the experiment the path length of the pump was held constant and the squeezed path was locked to either the squeezed or anti-squeezed quadrature using a method that combined the microcontroller locking algorithm [49] and the quantum noise locking method [66]. This method used a spectrum analyser set to a span of zero to demodulate the detected squeezed signal at 1MHz with a resolution bandwidth of 300kHz and video bandwidth of 1kHz. The external video output was then used as the error signal to control the squeezed beam path length with the microcontroller locking algorithm. The sampling frequency of the locking algorithm was set to 10kHz with a step size of around 2mV. As to be expected this locking method was unreliable and would occasionally drift from the squeezed quadrature due to the sharpness of the error signal. Due to time constraints this was the only method that could be quickly adapted to lock to the quadratures in this experiment.

[1] For an inference fringe between the signal and LO the fringe visibility from photodetector measurements is given by $\frac{i_{\max}-i_{\min}}{i_{\max}+i_{\min}}$ where i is the photocurrent

3.3 Results and Discussion

The OPA is a work in progress but has so far produced 11 dB of squeezing when corrected for dark noise as shown in Fig. 3.4. The total intra-cavity loss of 0.3% was measured and attributed mainly to the nonlinear crystal. This was measured using a high finesse cavity and comparing the calculated finesse of the cavity without the crystal to the measured finesse with the crystal. Using the measured cavity parameters a normalized pump parameter of $\beta_{\mathrm{n}} = 0.96$ was inferred. The theoretical curves of the squeezed and anti-squeezed quadratures from Eq. (2.45) using these parameters are plotted along side the measured traces in Fig. 3.4. With the poor mode matching of the pump to the cavity mode the first attempt to measure the squeezing spectrum only achieved 9 dB of squeezing. A second attempt with better mode matching resulted in 11 dB. The difference between the two recorded squeezing levels is likely due to the poor locking technique introducing noise into the measurement of the squeezed quadrature from the anti-squeezed quadrature rather than loss. This result falls short of the predicted 13dB from the measured parameters. To reach 13 dB of squeezing each locking loop in the experiment will be required to be carefully optimized to minimize noise. To measure greater than 15 dB the intra-cavity losses will need to be improved. To further characterise the OPA, the pump threshold power was measured. This was done by injecting a seed into the cavity and measuring the OPA gain while sweeping the pump power. The results of these measurements are shown in Fig. 3.5. This measurement was only made for the amplification gain. Despite best practice for experimental physics each data point was only recorded once so no meaningful error bars can be found for this data. However, two sets of measurements were made as shown in Fig. 3.5 showing the data is repeatable. From fitting the data the pump threshold power was found to be 624mW with a maximum regenerative gain of 1420. The predicted pump threshold power was calculated to be 685mW. This value was calculated with the non-linear interaction $\Lambda = 271$ found using manufacturer supplied parameters and measured parameters from the SHG cavity. The discrepancy between the predicted and measured values is mostly likely due to a better alignment of the ppKTP crystal inside the OPA cavity and hence the actual non-linear interaction strength is higher than in the SHG system.

More time will need to be invested into the method used to lock the homodyne detector to the squeezed and anti-squeezed quadratures. This will improve the observable squeezing. As it stands the current method requires patience for the microcontroller lock to stay locked on the correct quadrature for long enough to take a measurement. To try to reduce the fluctuations in the squeezed spectrum from the bad locking the data in Fig. 3.4 is averaged over 10 sweeps. Two other methods of locking are typically used here, chop

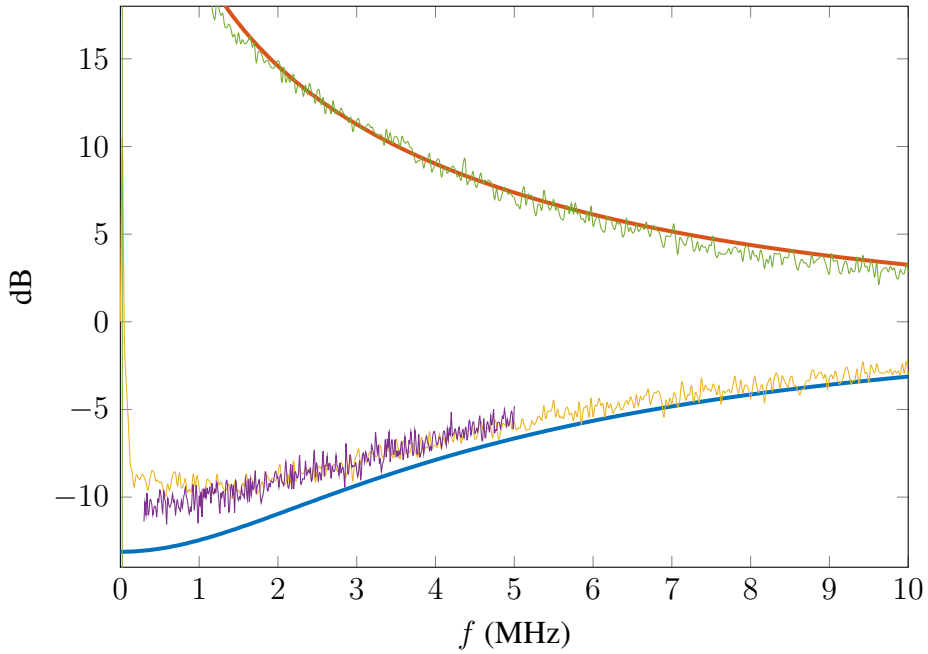


Figure 3.4: Plot of quadrature variance of the squeezed light from the OPA. The squeezed quadrature was measured with a poorly mode matched pump (yellow) and then again with the pump optimally mode matched (purple). The anti-squeezed quadrature (green) was measured with the poor mode matching but demonstrated a normalised pump parameter of $\beta_{\mathrm{n}} = 0.96$. Each trace was recorded using a spectrum analyser with a 30kHz resolution bandwidth and 1kHz video bandwidth. Eq. (2.45) is plotted for both the squeezed (blue) and anti-squeezed (red) quadratures using the measured loss of the non-linear crystal. A maximum squeezing of 13 dB is predicted for this OPA.

locking and coherent locking. Chop locking cycles a seed on and off either using AOMs or an optical chopper. The seed is provided long enough to stabilize the cavity and homodyne locks. The control signals are then held when the seed is removed [47]. Coherent locking uses a frequency shifted beam locked in phase with the pump to lock the homodyne to a quadrature [67]. The scheme can either be built using a pair of AOMs to provide the frequency shifted beams [68] or a second auxiliary laser.

The motivation for pursuing highly squeezed and pure CV states comes from their application to advanced quantum protocols and error correcting codes. One of the protocols only accessible with a low intra-cavity loss OPA is discussed in Ch. 7. Another obvious application for highly squeezed state is in error correction. For error correction to be successful it has to guarantee a low probability of failure. In quantum computing this probability relates to the reliability of the computations being performed. To phrase this another way, what would be the minimum level of squeezing required to perform reliable quantum computing? So far the answer to this question is 20.5dB [69]. Though it is expected that other protocols and QEC will appear with a requirement for less squeezing.

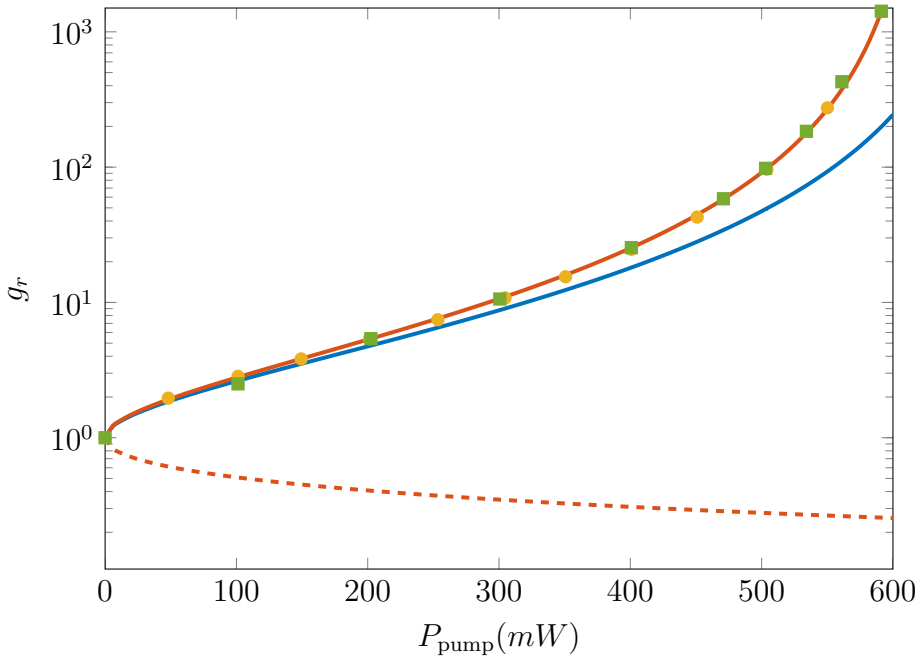


Figure 3.5: A plot of the pump power vs the regenerative gain. Two separate measurements were taken of the regenerative gain while sweeping the pump power (yellow and green). A curve was fitted (red, solid) to the measurements to give a pump threshold power of 624mW. The expected deamplified gain is also plotted as the red dashed line. The calculated pump threshold power was greater than the measured value (blue).

The main goal of the observation of the record breaking 15dB is to increase the sensitivity of the GEO 600 interferometer for gravitational wave detection [56]. A 10 dB enhancement would require less than 10% photon loss in the squeezed field. Another novel application from Ref. [56] was to use the highly squeezed states to calibrate the quantum efficiency of a photodiode. For their particular diode they measured an efficiency of 99.5% with an uncertainty of 0.5% without the need for a calibrated light source.

High levels of squeezing can also be used to provide incrementally improved results. One project lined up will combine a squeezing gate [70, 71] with a measurement based NLA [72] to create a probabilistic squeezed gate. It is expected that with the NLA the squeezed gate will be able to achieve a fidelity of 1 for higher levels of squeezing than was achievable in the original experiment [73].

3.4 Conclusion

In summary this chapter presented the current state of the development of a low intracavity loss OPA. The maximum observed squeezing after correcting for dark noise was 11 dB. With improvements to homodyne quadrature locking and stabilizing the optical

phase carefully, it should be possible to achieve the predicted 13dB of squeezing with the current cavity design. With a further reduction in the intra-cavity losses down to 0.1% from better anti-reflection coatings it is theoretically possible to generate 15dB of squeezing using the current experimental setup. Once optimised this design will serve as a platform for state generation in future experiments by the group on mirror position estimation and probabilistic squeezed gates.

Chapter 4

A Continuous Variable Bell Test

4.1 Introduction

A Bell test as discussed in Sec. 1.2 is a fundamental demonstration of quantum mechanics with applications in quantum technologies such as QKD and QRNG [18]. Using discrete variable quantum optics there have been to date four successful violations of a Bell inequality [4–7]. However, for CV quantum optics the challenge is much harder. As Bell argued in in Ref. [74] a violation of a Bell inequality with a state described by a positive Wigner function such as a CV EPR state would be impossible. There have been several protocols proposed which try to use more exotic CV states with photon subtraction [75] or using photon-wave correlations [76]. However, it was shown in Ref. [77] that in fact it is possible to violate a Bell inequality with EPR states using CV measurements provided one trusts the measurements. There are experiments going back over 35 years [25] and have been limited by non-deterministic quantum state resources and low quantum efficiency detection. The historical Bell tests relied on the "fair-sampling" assumption due to the limited quantum efficiency of single photon detectors. High quantum efficiency single photon detectors at cryogenic temperatures have recently been developed making loophole-free DV Bell tests possible. Using CV systems bring the advantage of well developed high efficiency large bandwidth detection at room temperatures as well as deterministically generated quantum states. This chapter presents the results from an experimental violation of a Bell inequalty of $B = 2.31 \pm 0.02$ based on the proposals of Ref. [77, 78]. This opens new possibilities of using CV states for device independent quantum protocols like those seen for DV.

This chapter is organised as follows. The proposals for a CV Bell test in Ref. [10, 78] will be reviewed in Sec. 4.2. Sec. 4.3 will discuss the modelling of the experiment and the considerations made. The experimental details are given in Sec. 4.4. The results and discussion of the experiment are given in Sec. 4.5.

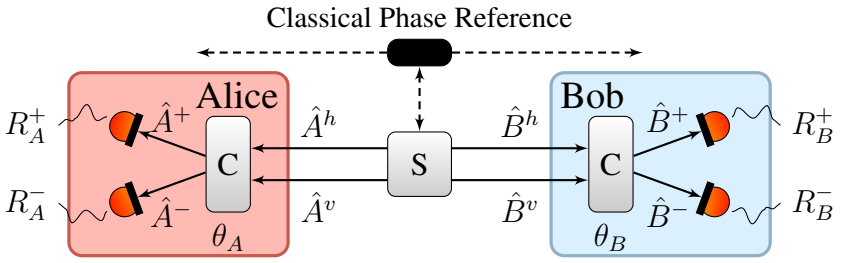


Figure 4.1: A diagram of a two channel CHSH Bell test.

4.2 Theory

The Bell test presented in this chapter is based on the two channel variation, depicted in Fig. 4.1, of the Bell test described in Sec. 1.2. Here the source, S, generates a four mode correlated optical state; two parties Alice and Bob are then given two modes each, $\hat{A}^h$, $\hat{A}^v$ and $\hat{B}^h$, $\hat{B}^v$ separated in polarization. They can mix their two modes to perform one of two measurements, $\{\theta_A, \theta'_A\}$ and $\{\theta_B, \theta'_B\}$, on their modes. Measuring the resulting modes $\hat{A}^+$, $\hat{A}^-$, $\hat{B}^+$ and $\hat{B}^-$ with single photon detectors will give one of two outcomes, $R \in \{0, 1\}$. Repeating this experiment a number of times Alice and Bob can build up correlation statistics between each others measurement outcomes with,

$$R(\theta_A, \theta_B)^{ij} = \langle R_A^i(\theta_A) R_B^j(\theta_B) \rangle, \tag{4.1}$$

where $i, j \in \{+, -\}$. The expectation value of the correlations for each of the four combination of measurement settings is given by.

$$E(\theta_A, \theta_B) = \frac{R^{++}(\theta_A, \theta_B) + R^{--}(\theta_A, \theta_B) - R^{+-}(\theta_A, \theta_B) - R^{-+}(\theta_A, \theta_B)}{R^{++}(\theta_A, \theta_B) + R^{--}(\theta_A, \theta_B) + R^{+-}(\theta_A, \theta_B) + R^{-+}(\theta_A, \theta_B)}. \tag{4.2}$$

These expectations can then be used to form the CHSH inequality [23],

$$B = |E(\theta_\mathrm{A}, \theta_\mathrm{B}) + E(\theta'_\mathrm{A}, \theta'_\mathrm{B}) + E(\theta'_\mathrm{A}, \theta_\mathrm{B}) - E(\theta_\mathrm{A}\theta'_\mathrm{B})| \leq 2. \tag{4.3}$$

A maximal violation of the inequality can be observed with measurement settings $\theta_A = \{\frac{\pi}{8}, \frac{3\pi}{8}\}$ and $\theta_B = \{0, \frac{\pi}{4}\}$.

The continuous variable Bell test proposals in Ref. [77, 78] are based around an entanglement source using OPA's and homodyne measurements. The photon correlations needed for a Bell test are inferred through quadrature measurements using the equivalence

$$\hat{A}^\dagger \hat{A} \equiv (\hat{A}^\dagger \hat{A} - \hat{V}^\dagger \hat{V}) = \frac{1}{4}(\hat{X}_A^2 + \hat{P}_A^2 - \hat{X}_V^2 - \hat{P}_V^2), \tag{4.4}$$

for a mode $\hat{A}$. Here $\hat{X}_F$ and $\hat{P}_F$ are the quadrature operators for the mode $F \in \{A, V\}$, where V is the vacuum mode with the corresponding creation operator $\hat{V}^\dagger$. The measurement of the background vacuum is inherent in homodyne measurement. Typically the quandrature measurements made by a homodyne detector are normalised by the power in the local oscillator. In Eq. (4.4) the local oscillator mode is equivalently subtracted from the quadrature modes. This of course is not practical as the vacuum needs to be measured separately but the equivalence can be used to find a correlation function that can be measured. A direct measurement in the Fock basis of the detected field will yield Eq. (4.4).

If Alice and Bob consider the photon number in each detected mode the correlation equation Eq. (4.1) becomes,

$$R^{ij} = \langle \hat{A}_i^\dagger \hat{A}_i \hat{B}_j^\dagger \hat{B}_j \rangle. \tag{4.5}$$

Using the equivalence relation Eq. (4.4), the correlation Eq. (4.1) can be rewritten again to be in terms of homodyne measurements of the quadratures. By assuming Gaussian statistics, all correlations can be reduced to second order correlations. In this case, using $\langle \hat{X}^2 \hat{Y}^2 \rangle = \langle \hat{X}^2 \rangle \langle \hat{Y}^2 \rangle + 2\langle \hat{X}\hat{Y} \rangle^2$, to get,

$$\begin{aligned} R^{ij} =& \frac{1}{16}[2(\langle \hat{X}_A^i \hat{X}_B^j \rangle^2 + \langle \hat{P}_A^i \hat{P}_B^j \rangle^2 + \langle \hat{X}_A^i \hat{P}_B^j \rangle^2 + \langle \hat{P}_A^i \hat{X}_B^i \rangle^2) \\ &+ V_{A;X}^i V_{B;X}^j + V_{A;P}^i V_{B;P}^j + V_{A;P}^i V_{B;X}^j + V_{A;X}^i V_{B;P}^j \\ &- 2V_v(V_{A;X}^i + V_{A;P}^i) - 2V_v(V_{B;X}^j + V_{B;P}^j) \\ &+ 4V_v^2]. \end{aligned} \tag{4.6}$$

Here $V_{m:n}^i$ the variance of the measurement made by party $m = \{A, B\}$ in the quadrature $n = \{X, P\}$. The variance V_v is the variance of the measured vacuum but could also be considered to represent the noise on the vacuum measurement. Eq. (4.6) shows how the photon number correlation can be inferred from the Gaussian homodyne measurements.

To see how Eq. (4.6) can be used to produce a Bell violation the significance of each term is considered. The first four terms are dependent on the measurement angle with the next four being polarization independent. The last three terms come from the quantum noise of the vacuum state. In a perfect experiment the polarization independent terms will cancel with the quantum noise terms to create high correlation fringe visibility with respect to θ_A and θ_B. This fringe visibility can be diminished by the measurement of uncorrelated photons from classical noise sources and high order photon number terms such as those in highly entangled CV states. In a purely classical experiment the last three terms will be zero and result in a small correlation fringe. The correlation function Eq. (4.6) can then be used to bound the measured expectations between Alice and Bob

with the Bell inequality Eq. (4.3).

In regards to this protocol it is assumed that the contribution of the vacuum mode will be such that $\langle \hat{V}_v^\dagger \hat{V}_v \rangle = 0$ to meet the requirement that Eq. (4.4) remains a positive operator. If this assumption is violated it opens loopholes that could explain a Bell violation from this protocol. To rule out this loophole the photon number count for the V mode, i.e. with all the light blocked, n_{dark}, should be much less than the photon number count in the local oscillator, n_{LO}. In particular $n_{\text{dark}} \ll \sqrt{n_{\text{LO}}}$. This test demonstrates that the homodyne measurements are truly of vacuum correlations. It is well established by many experiments that this is a good assumption at optical frequency side bands. However this requires trust of the detection device.

4.2.1 CV Bell state source

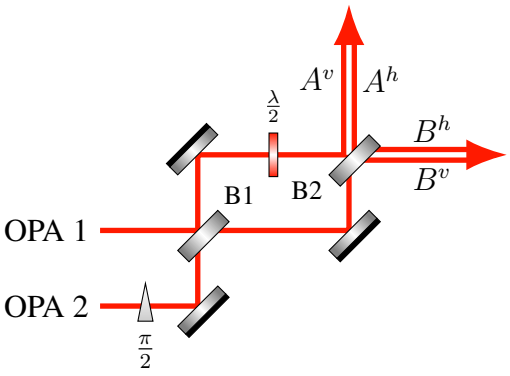


Figure 4.2: The chosen Bell state source. Squeezed states produced by OPA 1 and OPA 2 are shifted to be in othogonal quadratures. They are then mixed on a 50/50 BS (B1). The resulting beams are then shifted into opposite linear polarisations before being mixed on a second 50/50 BS (B2). This creates four output modes, A^h, A^v, B^h and B^v, that make up the Bell state.

To observe a violation of Eq. (4.3) with the correlation function Eq. (4.6) a CV source is required to produce the Bell state. For this experiment the second source proposed in ref. [78], shown in Fig. 4.2 was chosen. This source is based on the well known Bell test performed by Ou and Mandel [79]. Rather than post selecting entangled photons by photon counting as in the Ou Mandel experiment, the CV correlations of a similar state are analysed according to Eq. (4.6). In this experiment the CV source the entangled state is created by interfering two orthogonal squeezed states on a 50/50 BS (B1). To create the Bell state the entangled modes are shifted into orthogonal linear polarization and then mixed on a second 50/50 BS (B2). These four modes are then distributed to Alice and Bob. Of the three proposals analysed in ref. [78] the one selected performs the worst however it is by far the simplest in terms of experimental complexity.

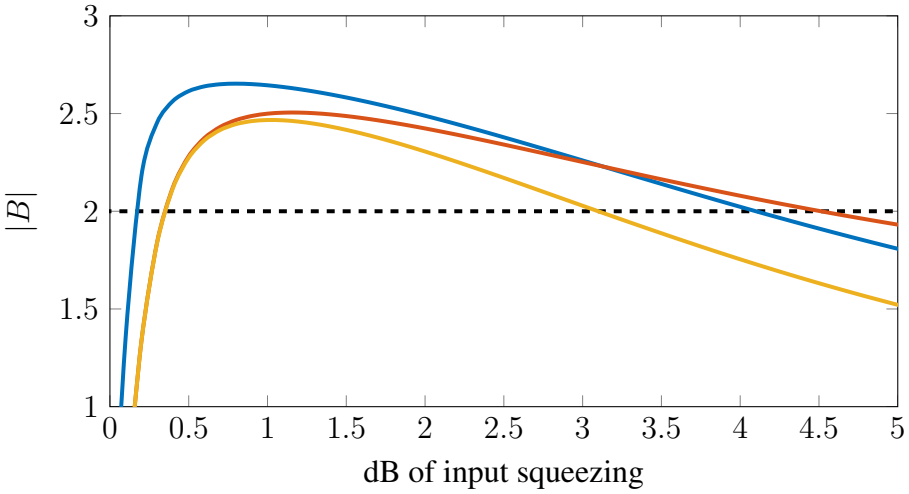


Figure 4.3: Comparison of the three proposed schemes for a CV Bell test with 0.95 detection efficiency and dark noise 18dB below shot noise. The yellow line is the chosen scheme, shown in Fig. 4.2. The blue line is the original source proposed in Ref. [77] and the red line is the first source proposed in Ref. [78].

4.3 Modelling

Using the Gaussian assumption made for Eq. (4.6) a model can be made using the phase state representation discussed in Sec. 1.4. Both the input state, γ_{in}, and the output state, γ_{out} can be represented by four modes. This means both states can be represented by an 8 by 8 covariance matrix. Here it is assumed that the mean vector will be zero. The matrix γ_{in} was constructed such that each sub matrix γ_{out}^{ij}, where $i, j \in 2n-1, 2n$, represents the two quadratures for one of the four measured modes indexed by n. Each element in this experiment is applied using a sympletic operation to get an expression for γ_{out} in terms of γ_{in}. The sympletic operator representing the experiment is given by

$$S = S_{\theta_{\text{B}}}^{1,3} S_{\theta_{\text{A}}}^{1,3} S_{B2}^{2,3} S_{B2}^{1,3} S_{B1}^{1,2}. \tag{4.7}$$

The input state is simply given by the diagonal matrix,

$$\text{diag}(\gamma_{\text{in}}) = \left[V_{\text{sqz}}^{\text{opa1}} \quad V_{\text{asqz}}^{\text{opa1}} \quad V_{\text{sqz}}^{\text{opa2}} \quad V_{\text{asqz}}^{\text{opa2}} \quad 1 \quad 1 \quad 1 \quad 1 \right], \tag{4.8}$$

where V_{sqz} is the variance of the squeezed quadrature and V_{asqz} for both OPA 1 and OPA 2. To add the contribution of detector efficiency, η, and noise relative to the output, ε, a completely positive map was used to arrive at,

$$\gamma_{out} = \sqrt{\eta}\mathbb{I} S \gamma_{in} S^T \sqrt{\eta}\mathbb{I} + \varepsilon\mathbb{I} \tag{4.9}$$

This model will account for the case where OPA 1 and OPA 2 are not symmetric. To arrive at Fig. 4.3 and Fig. 4.4 the model was simplified so that the input state became,

$$\mathrm{diag}(\gamma_{\mathrm{in}}) = \left[V \quad \tfrac{1}{V} \quad V \quad \tfrac{1}{V} \quad 1 \quad 1 \quad 1 \quad 1\right], \tag{4.10}$$

where V is variance of the squeezing produced by OPA 1 and OPA 2.

This model was fitted to each of the experimentally obtained values of R^{ij} using an iterative fitting process to find η, ε, V_{asqz} and V_{sqz}. The measured parameters provided the starting point for the fitting algorithm. Using this fitting process gave a better prediction of the output correlations than when the measured values were used in the model.

4.3.1 Experimental considerations

The correct measurement of shot noise in this experiment is crucial to this Bell test. Particularly in ensuring Eq. (4.4) remains a positive operator. The shot noise was found to drift up to 1% over the course of a run of this experiment. Incorrectly measuring shot noise can lead to spurious violations of Eq. (4.3) for unentangled states. To see this effect consider Eq. (4.6) where the data is normalized to the shot noise CV_V. Here C is a constant to represent the effect of dark noise contaminating the shot noise variance. The first eight terms in Eq. (4.6) will now have a factor C^2, the next two will have a factor C and the last term will remain unaffected. This will reduce the cancellation between the polarisation independent terms and the quantum noise terms but more importantly it will artificially increase the first four correlation terms producing an overall increase in Bell violation. The change in the Bell violation is shown in Fig. 4.4

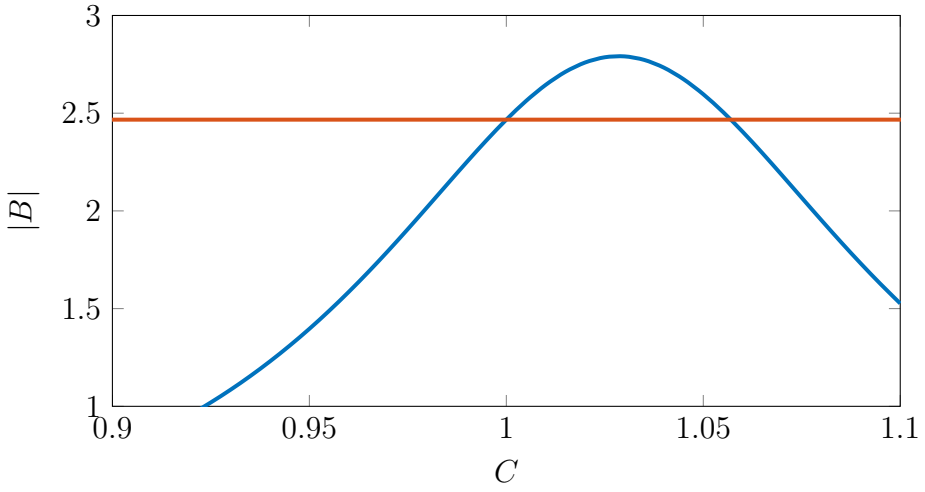


Figure 4.4: Effect of incorrect normalisation with 1 dB input squeezing and 18 dB clearance between darknoise and shot noise.

Modelling of the experiment with this source shows several important factors that could reduce the Bell violation [78]. Underlying this Bell test is essentially a single photon experiment and as such the inequality will be maximally violated when the source mostly produces correlated pairs of single photons. An important parameter is then the input squeezing; with high levels of input squeezing the Bell violation decreases. As shown in Sec. 1.3.3, squeezed states are made up of photons in sets of multiples of two with a decreasing probability. Increasing squeezing of a state will increase the probability of the higher order photon terms occurring. These higher order photon number terms can introduce correlations that dilute the Bell correlations and decrease the violation. Any noise in the experiment will have the same effect of decreasing the violation though by decreasing the correlations. The two main sources of noise for this experiment were identified as the input state purity and detector dark noise.

Just as in the single photon equivalent experiment loss will increase the number of samples required to get a significant correlation value. This is not really a concern for this experiment given the deterministic resources and high bandwidth detection. The loss can however also decrease the violations by increasing the effect of noise that appears at the output such as detector dark noise.

4.4 Experiment

A schematic of the experiment is shown in Fig. 4.5. The squeezed states are created in the side bands of spatially separated beams of a Nd:YAG 1064nm laser. The side bands were squeezed using two singly resonant bow tie cavity OPAs each containing a 1cm long periodically pold Potassium Titanyl Phosphate (ppKTP) crystal. Both of the OPAs were seeded by the 1064nm laser. A second harmonic generator provided a 532nm source to pump the ppKTP crystals and create the squeezed light. The two squeezed beams are mixed in quadrature on B1. Two slightly reflecting glass slips were used to create an error signal from the coherent interference. This error signal was used to control P1 to lock the squeezed beams in quadrature.

The entangled beams are then separated in polarisation by a halfway plate before being interfered on B2. The resulting modes of $\hat{A}^h$, $\hat{A}^v$, $\hat{B}^h$ and $\hat{B}^v$ are then sent to Alice and Bob accordingly. As this experiment is derived from a discrete variable Bell test the result should be invariant to relative phase between each beam path between B1 and B2. However it is necessary to lock each homodyne detector to orthogonal quadratures. To do this the experiment used two phase modulations applied separately to the OPAs for PDH locking. The phase between each of the beam paths was controlled by a piezo controlled mirror, P2, to hold the modulations orthogonal to each other. As the distance

between B1 and B2 was so small P2 was not required to be actively locked and was manually controlled. An additional quarter wave plate ($\lambda/4$) was used to correct for a phase mismatch between $\hat{A}^h$ and $\hat{A}^v$ caused by B2. Both B1 and B2 are 50:50 beam splitters.

To find the set point for P2 the phase between the two locking signals was observed on Bob's detectors with $\theta_B = \pi/2$. The position of mirror P2 was adjusted until one of the two signals had maximised and the other minimized which corresponded to the locking signals being orthogonal. This unfortunately created a situation where only one of the two locking signals could be used to locking Bob's homodynes with $\theta_B = \pi/2$. To lock to the other quadrature the DC subtracted signal was used.

To mix Alice's and Bob's modes a halfwave plate was used to rotate the polarisation by an angle before being mixed on a PBS to create the modes A^+, A^-, B^+ and B^-. To measure the correct shot noise an optical beam chopper was positioned after B2 was used to switch the homodyne detectors between measuring the signal and shot noise. This reduced the requirement on the stability of the experimental setup. The shot noise and signal were divided up in post processing.

To highlight the difficulty in this experiment there has been an attempt to include the electronics in Fig. 4.5. The homodyne locking was done using locking method described in Sec. 2.4.2 [46]. The use of this locking code made this experiment possible by significantly increasing the speed at which the experiment could be conducted. The initial experimental runs took around two hours to compete. This was due to the number or measurements required and the frequent sampling of shot noise. After modifying the code to automatically switch measurement quadratures and record data with the beam chopper running, the experiment only took 30 minutes to complete. The reduction in time to conduct the experiment was important to the results as it was shown early on that the experiment had a significant drift.

From modelling it was found the maximal violation for the experiment would occur with both OPA's generating approximately 1 dB of squeezing with a measured dark noise of 18 dB below shot noise for the homodyne detectors.

4.4.1 Detection protocol

A set of four fixed measurement settings were identified that would give all the correlation and variance terms required by Eq. (4.6). These measurements were made in a fixed order for each combination of θ_{A}, θ'_{A}, θ_{B} and θ'_{B} with the shot noise regularly sampled using the beam chopper during measurements. The dark noise measurement was only taken once at the end of each experimental run. To keep the experiment to a single optical table the

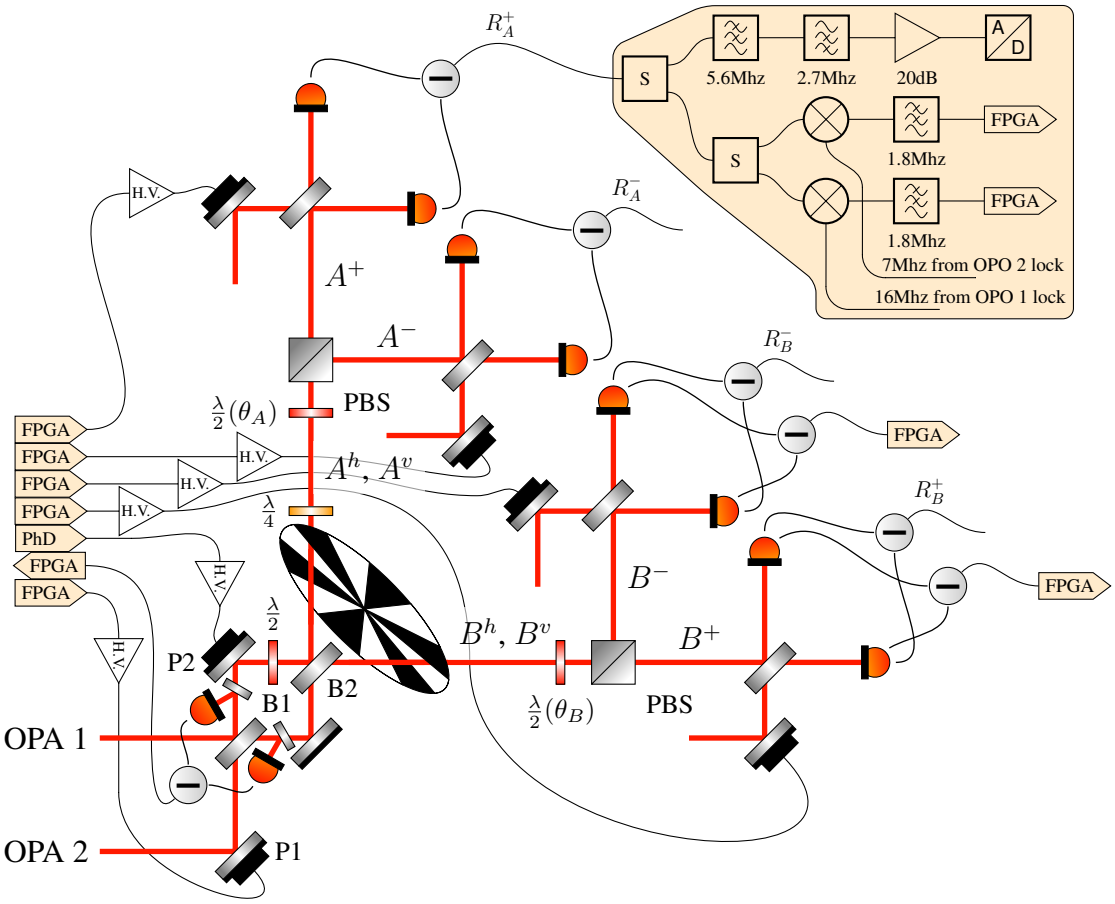


Figure 4.5: A schematic diagram of the experiment. The Bell state is generated by mixing two orthogonal squeezed states in the same linear polarization on a 50:50 BS to generate an EPR state. One arm of the EPR state is rotated into the orthogonal polarization. The two beams are then interfered on a second BS. This results in the generation of four correlated modes; $\hat{A}^h$, $\hat{A}^v$, $\hat{B}^h$ and $\hat{B}^v$ separated spatially and in polarization from two quadrature squeezed states. Alice and Bob each receive two polarization separated modes and mix their polarisation by θ_A and θ_B respectfully. As a result of the birefringence of BS2 the modes $\hat{A}^h$, $\hat{A}^v$ were not orthogonal. This was corrected with a $\lambda/4$ plate. The resulting modes; $\hat{A}^+$, $\hat{A}^-$, $\hat{B}^+$ and $\hat{B}^-$ are measured with homodyne detectors. The measurements filtered and amplified before (yellow box) being recorded via a digitizer connected to a computer. Each phase lock was controlled using the controller described in Sec. 2.4.2 running on a FPGA. An optical beam chopper was used to switch between making a quadrature measurement and measuring shot noise.

detectors were located next to each other and sampled using the same digitizer.

4.5 Results & Discussion

The main result presented in this chapter is the violation of Eq. (4.3) with $B = 2.31$ with a standard deviation of 0.02 using 1.1 dB of input squeezing. The violation of Eq. (4.3) was also demonstrated with squeezing of the input fields up to 1.8 dB. Sweeping of the input squeezing with both OPA's in Fig. 4.6 shows the effect of increasing the anti-squeezing noise on the experimental setup. As the OPA's are pumped harder to produce more squeezing the purity of the state they produce decreases due to more noise in the anti-squeezed quadrature. From a model fitted to the data, described in Sec. 4.3, it was found the purity decreased from 0.98 for 1.1 dB of squeezing to 0.92 for 3.9 dB of squeezing. The results from Ref. [78] and Fig. 4.3 show that for a similar detector noise it should be possible to observe a Bell violation for up to 3 dB of squeezing, a result not observed in this experiment due to the decreasing purity of the squeezed states. A second experimental run was conducted where the local oscillator power was decreased for each homodyne detector to simulate the effect of an increase in detector dark noise. This gave the expected result of a decrease in violation of Eq. (4.3).

4.5.1 Correlation fringes

A third experimental run was conducted to observe the correlation fringe. To do this θ_A was fixed at $\pi/8$ while θ_B was swept from 0 to $\pi/2$ rad. The input squeezing was set to be 1.1 dB. The correlation fringes from this experiment are plotted in Fig. 4.7 (b) as normalized P values. The P values are calculated with

$$P^{ij} = \frac{R^{ij}}{\sum_{i,j} R^{ij}}. \tag{4.11}$$

The correlation fringe visibility was measured to be over 75%. This could be further improved by reducing the noise in the experiment. From the normalized P values a comparison is made with the recorded homodyne data plotted in Fig. 4.7 (a) with the corresponding Pearson correlation. For the raw homodyne data a very weak correlation is observed but from this a significant P value is still observed. The process of calculating B is given a visual representation by reading Fig. 4.7 from left to right. The homodyne correlations and variances are used to calculate the photon correlations and then the expectation value for each measurement setting.

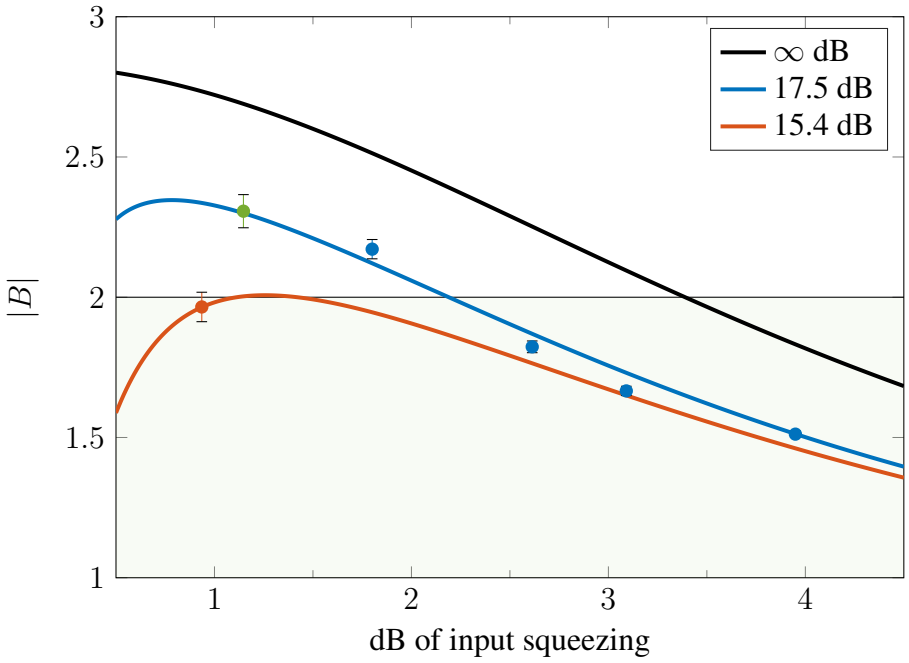


Figure 4.6: Bell violations showing the effect of different experimental parameters. The highest recorded value was $B = 2.31$ (green point) with 15 standard deviations above the classical limit (shaded region). The detector dark noise was measured to be 17.5 dB below shot noise. The Bell violation decreases as the input squeezing generated by OPA 1 and OPA 2 is increased (blue points). A decrease in the dark noise clearance of the homodyne detectors to 15.4 dB was created by decreasing the local oscillator power. As expected the value of $|B|$ (orange point) decreased below 2. The error bars shown are three standard deviations from the mean violation as found with random re-sampling of the data. The model from Sec. 4.3 was fitted to the data as described in Sec. 4.5.2 to infer the experimental parameters. The fitting found detector losses of 10% and a state purity that decreases from 0.98 to 0.92 as the squeezing is increased from 1.1 dB to 3.9 dB for the detector dark noise clearances of 17.5 dB (blue line) and 15.4 dB (red line). For comparison the theoretical upper limit of B for the experiment has been included with infinite dark noise clearance, no loss and pure input states (black line). The shift in the peak of the Bell violation is due to the input squeezing from OPA 1 and OPA 2 being unmatched

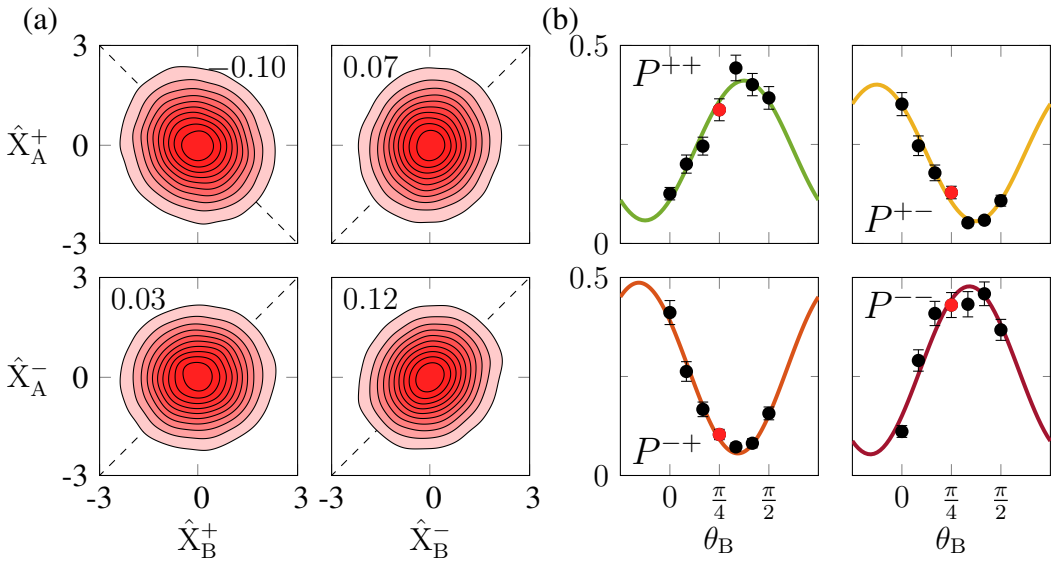


Figure 4.7: Raw homodyne data correlations with the photon correlation fringes and expectation values vs θ_B with 1.1dB input squeezing and $\theta_A = \pi/8$. The weak correlations in the homodyne data, represented in topographical maps with the Pearson correlation displayed (a), translates to strong photon correlation fringes, (b) with the recorded visibility above 75%. The correlations are then used to find the expectation fringe Fig. 4.8. The error bars are three standard deviations away from the mean correlation value of repeated random samples of the recorded data.

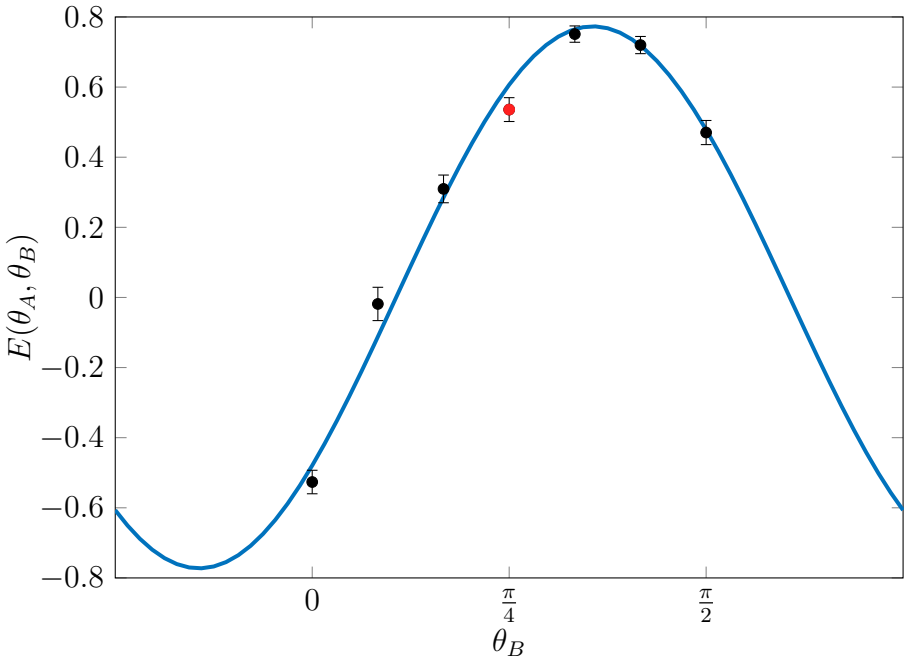


Figure 4.8: The expectation fringe found using the correlation fringes in Fig. 4.7 (b).

4.5.2 Fitting the model

For Figs. 4.6 to 4.8 the model described in Sec. 4.3 was fitted to the experimental data using an iterative fitting process. The starting parameter for the fit were $V_{\mathrm{asq}} = 1.25$, $V_{\mathrm{sqz}} = 0.79$, $\eta = 0.95$ and $\xi = 10^{-1.8}$. The fit gave a better prediction of the output correlations than when the measured values were used in the model. This was partly due to the fitting being able to capture the contributions in noise and losses from the optical components and locking.

4.6 Conclusion

In this chapter the results of the first observation of Bell correlations in a continuous variable system have been presented with a violation of 2.31 at 15 standard deviations above the classical limit with a detector dark noise of 17.5dB below shot noise. This result demonstrates the strength of photon number correlations when inferred through homodyne measurements. A demonstration of a violation of the Bell inequality was also made with 1.8 dB of input squeezing and would be possible to up to 2 dB of input squeezing with this experiment. These correlations exist between side-band modes of a bright beam that would be very difficult to measure directly via photon counting. This result was possible because of the high correlation fringes observed with this experiment. While this Bell test fails to address any loopholes it is still a significant result. In order for this violation to be believed the detection devices must be trusted due to the hard to close loop-hole caused by the shot-noise verification. Never-the-less this Bell test could be applied to a source independent QRNG similar to those protocols proposed in Ref. [80, 81].

Part II

Continuous Variable Quantum Key Distribution

Overview

The idea that quantum mechanics could be used for cryptographic applications dates back to 1983 when a publication proposed that a series of quantum states could be stored on a bank note to prevent forgery. Each state was created in one of two basis. An adversary not knowing which basis was used to create each state would not be able to perfectly measure the states on a bank note. As was shown in Ch. 1 measuring a state in the wrong basis would introduce errors in the measurements. An attempt to create a copy of the note it would be easily detected by the bank which would know perfectly which measurements would be required to retrieve each state and any errors present would be detected. In fact due to the no-cloning theorem, quantum mechanics limits the fidelity between a clone and the original quantum state [82, 83]. The idea for quantum money never gained traction but influenced the idea of using quantum mechanics as solution to the cryptography problem of key distribution [84]. The first proposed quantum key distribution protocol was published in 1984 with much more success [14]. Since then there have been numerous proposals for QKD protocols using both CV and DV approaches [28, 85]. Another application of quantum mechanics in cryptography comes from its thirst for high quality random numbers for encryption keys. As measuring quantum states is inherently random this is a natural application. Of course these random numbers can also be applied in many other areas including gaming, simulations [86] and even art [87].

The following chapters build on the ideas presented in Part I and present a proposal for a better way of characterising Eve and the results from a one sided device independent QKD protocol demonstration. Ch. 5 will be a brief description and introduction into Shannon information and quantum information to provide the mathematical framework required for the subsequent chapters. This chapter will also give an introduction to quantum random number generation and quantum key distribution. Ch. 6 covers a proposal published in Ref. [88] for estimating an adversaries information using a combination of commonly used parameter estimation methods. Ch. 7 will report on a proposal and experiment published in Ref. [17] for family of one-sided device independent CV QKD protocols.

A good introduction to quantum communications is given in Ref. [13]. This book covers both classical and quantum information and provides an introduction to DV QKD. For CV QKD a very complete description of the Gaussian CV QKD protocols discussed in Ch. 5 to 7 is found in Ref. [29]. For general reading on cryptography Ref. [84] gives a well presented history and motivation behind cryptography.

Chapter 5

Background Theory

5.1 Shannon Information

Information theory has contributed greatly to technological development and has found its way into many different scientific and engineering disciplines. It has helped to greatly change the way we communicate from when it was first proposed by Claude E. Shannon in 1948 [89]. Information theory provides a mathematical framework for the quantisation of information using Shannon entropy to measure the information of a random variable. The entropy of a random variable X is given by,

$$H(X) = -\sum_x p_x \log_2 p_x, \tag{5.1}$$

where p_x denotes the probability of X having the outcome x. As an example consider X to be the outcomes of a coin flip with equal probably of head or tails, i.e. $p_{\text{Heads}} = p_{\text{Tails}} = 0.5$. This gives $H(X) = 1$ which can be interpreted as the variable X being maximally random. This same measure can be applied to other tasks such as data compression where one would like to know the minimum bits required to represent a file. Shannon entropy can be extended to multiple variables. Continuing the coin flipping example a second variable could be the previous coin flip, $Y \in \{\text{H}, \text{T}\}$. The joint entropy of X and Y is written as,

$$H(X, Y) = -\sum_{x,y} p(x, y) \log_2 p(x, y). \tag{5.2}$$

Of course if the coin flipping is truly random then X and Y will be independent and the joint entropy will be equal to the sum of their individual entropies. Another important measure in information theory is conditional entropy. That is, given a known outcome of a variable Y what is the uncertainty of X?

$$H(X|Y) = -\sum_{x,y} p(x, y) \log_2 \frac{p(x, y)}{p(y)}. \tag{5.3}$$

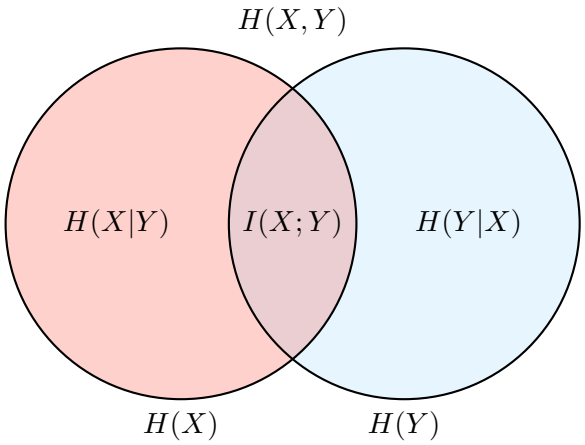


Figure 5.1: A Venn diagram representation of each information measure. The red circle represents $H(X)$ and the blue circle represents $H(Y)$. The relations here are given in Eq. (5.5)

For the coin flip example this could be interpreted as if the outcome of Y is known then how hard would it be to predict the outcome of X. The last entropy to be covered in this section is mutual information. That is, given the two random variables X and Y how much information can be gained from X by observing Y. In practice this is usually interpreted as the shared information between X and Y.

$$H(X;Y) = I(X;Y) = -\sum_{x,y} p(x,y) \log_2 \frac{p(x,y)}{p(x)p(y)}. \tag{5.4}$$

For the coin flip example the mutual information will be maximized if $X = Y$ and minimized if X and Y are completely independent. For Shannon entropies the mutual information is symmetric, $I(X;Y) = I(Y;X)$. The following relations between the mutual information, conditional entropy and joint entropy are useful to know for this thesis,

$$\begin{aligned} H(X|Y) &= H(X,Y) - H(Y) \\ I(X;Y) &= H(X) - H(X|Y) = H(X) + H(Y) - H(X,Y) \\ H(X,Y) &\leq H(X) + H(Y). \end{aligned} \tag{5.5}$$

These relations can be used to create the Venn diagram in Fig. 5.1.

5.1.1 Shannon Entropies of Gaussian states

The Shannon entropy is easily calculated for a variable X described by Gaussian distribution with variance σ^2 and a mean of 0,

$$H(X) = \frac{1}{2}\log_2 \sigma^2 + C, \tag{5.6}$$

where C is an arbitrary constant dependent on scaling. Extending this to a two mode state the joint Shannon entropy for the variables X and Y with covariance $C_{X,Y}$ described by the covariance matrix

$$\gamma = \begin{bmatrix} \sigma_X^2 & C_{X,Y} \\ C_{X,Y}^T & \sigma_Y^2 \end{bmatrix} \tag{5.7}$$

is given by

$$H(X,Y) = \frac{1}{2}\log_2 \det[\gamma] + C'. \tag{5.8}$$

Likewise the conditional entropy is,

$$H(Y|X) = \frac{1}{2}\log_2 \sigma_{Y|X}^2 + C, \tag{5.9}$$

where $\sigma_{Y|X}^2$ is the conditional variance given by,

$$\sigma_{Y|X}^2 = \sigma_Y^2 - \frac{C_{X,Y}}{\sigma_X^2}. \tag{5.10}$$

Finally the mutual entropy can be as written in terms of Eq. 5.8 or Eq. 5.9 with Eq. 5.6 using the relations in Eq. 5.1,

$$\begin{aligned} H(X:Y) = H(Y) - H(Y|X) &= \frac{1}{2}\log\frac{\sigma_Y^2}{\sigma_{Y|X}^2} \\ = H(X) - H(X|Y) &= \frac{1}{2}\log\frac{\sigma_X^2}{\sigma_{X|Y}^2} \\ = H(X) + H(Y) - H(X,Y) &= \frac{1}{2}\log\frac{\sigma_Y^2\sigma_X^2}{\det\gamma} \end{aligned} \tag{5.11}$$

5.1.2 Rényi entropy

Shannon entropy is included in the general family of entropic quantities called the Rényi entropies. The Rényi entropies are given by,

$$H_\alpha(X) = \frac{1}{1-\alpha}\log_2\left(\sum_{i=1}^{n} p_i^\alpha\right) \tag{5.12}$$

where $\alpha > 0$ and $\alpha \neq 1$. α is the order of the entropy with $\alpha = 0$ being know as the max entropy as it is always the largest of all the Rényi entropies. The Shannon entropy is the limit where $\alpha \to 1$. The limit where $\alpha \to \infty$ is known as the min entropy which is the negative log of the probability of observing the most likely value. This is of interest for random number generators where one wants to know how unpredictable the next value of a random process will be. The min entropy is,

$$H_\infty = \min_i(-\log_2 p_i) = -\log_2 \max_i p_i \tag{5.13}$$

5.2 Quantum Information

In the same way the information contained in classical state can be measured the information contained in a quantum state can be measured using von Neumann entropy. The description of von Neumann entropies in this section is made using the density operators of a state. The entropy of a state described by a density operator, ρ, is given by,

$$S(\rho) = -tr(\rho \log_2 \rho). \tag{5.14}$$

As with Shannon entropy the conditional, joint and mutual Von Neumann entropies can be defined as

$$S(A, B) = -tr(\rho^{XY} \log_2 \rho^{XY}) \tag{5.15}$$

$$S(A|B) = S(A, B) - S(B) \tag{5.16}$$

$$S(A : B) = S(A) + S(B) - S(A, B) \tag{5.17}$$

Not all the same properties carry over from Shannon entropy. An example of this is the conditional Shannon entropy is always greater or equal to 0. For von Neumann entropy the conditional entropy can be negative and is considered a representation of the presence of entanglement. There are a few von Neumann entropy properties that will be needed later in this thesis given below,

- $S(A) \geq 0$ where $S(A) = 0$ signifies a pure state,
- $S(A) = S(B)$ if $S(A, B) = 0$, and
- $S(AB) = S(AC)$ if $S(A, B, C) = 0$.

5.2.1 Holevo bound

The Holevo bound plays an important role in quantum information as it bounds the accessible information. This is an important bound for QKD. If Alice prepares a series of states ρ_x and Bob performs a measurement to receive the outcome Y the accessible information to Bob is bounded above by,

$$H(a:b) \leq S(a:B) = \chi(a:B) = S(\rho) - \sum_x p_x S(\rho_x), \tag{5.18}$$

where $\rho = \sum_x p_x \rho_x$ and $\chi(a:B)$ represents the Holevo quantity. Here classical states are written as lower case letters to distinguish them from quantum states represented by upper case letters.

5.2.2 von Neumann entropy for Gaussian and thermal states

A Gaussian state can be decomposed into a tensor product of thermal states. A covariance matrix γ representing a Gaussian state can be written as,

$$S\gamma S^T = \bigotimes_{k=1}^{N} \lambda_k \mathbb{I}, \tag{5.19}$$

where each $\lambda_k \mathbb{I}$ is the covariance matrix of a thermal state and λ_k is a symplectic eigenvalue of γ.

For a N mode thermal state, ρ the entropy is given by,

$$S(\rho) = \sum_{k=1}^{N} S(G(\lambda_k - 1)/2), \tag{5.20}$$

Where

$$G(x) = (x+1)\log_2(x+1) - x\log_2 x. \tag{5.21}$$

Symplectic eigenvalues

The symplectic eigenvalues for matrix γ are obtained by diagonalisation with a symplectic transform S as shown in Eq. (5.19). The symplectic eigenvalues can be easily found for one and two modes states.

One-mode normal decomposition For a single mode state the symplectic eigenvalue is simply given by the square root of the determinant of γ,

$$\lambda^2 = \det[\gamma]. \tag{5.22}$$

Two-mode normal decomposition For two modes finding the symplectic eigenvalues is a little more difficult. Consider the covariance matrix,

$$\gamma = \begin{bmatrix} \gamma_1 & C_{12} \\ C_{12}^T & \gamma_2 \end{bmatrix} \tag{5.23}$$

To find the symplectic eigenvalues the following two symplectic invariants can be defined,

$$\Delta = \lambda_1^2 + \lambda_2^2 = \det\gamma_1 + \det\gamma_2 \det C_{12}, \qquad \lambda_1^2\lambda_2^2 = \det\gamma. \tag{5.24}$$

The symplectic eigenvalues are the solution of the polynomial,

$$z^2 - \Delta z + \det\gamma = 0. \tag{5.25}$$

With the solution,

$$\lambda_{1,2}^2 = \frac{1}{2}\left[\Delta \pm \sqrt{\Delta^2 - 4\det\gamma}\right]. \tag{5.26}$$

5.2.3 Entropic uncertainty principle

The Heisenburg uncertainty principle was introduced in Sec. 1.3 as a lower limit in the variance of two non commuting variables e.g. amplitude and phase. The use of variance as a measure of uncertainty limits the tightness of the inequality to Gaussian distributed variables. The Heisenburg uncertainty principle can be reformulated in terms of entropy to give the entropic uncertainty principle (EUP) which is a tighter inequality [90]. The most well known of these uncertainties is [91],

$$H(X) + H(Z) \geq \log(\frac{1}{c}). \tag{5.27}$$

Here c is the maximum overlap between two eigenvectors of X and Z. This equality bounds the information in two discrete variables, X and Z. This naturally makes it unsusceptible to decreasing from changes in the labeling of measurement outcomes and noise due to the monotonicity of Shannon entropy. An application of interest of the entropic uncertainty is describing a tripartite guessing game where we have three parties, Alice, Charlie and Bob. A source will prepare a quantum state described by ρ_{ABC}. Bob and Charlie

store their states in separate quantum memories. Alice measures ρ_A in a randomly selected complementarity basis, X or Z. Bob and Charlie then have to independently guess Alice's measurement outcome given they have access to their state. Afterwards Alice announces which basis she measured. After a number or trials Alice, Bob and Charlie compare their results. Charlie and Bob win the game if they both guess Alice's measurement outcomes correctly. This is called the monogamy game as it is impossible for Bob and Charlie to ever win due to the monogamy of entanglement. If ρ_B is more entangled with ρ_A than ρ_C then Bob will have more certainty in his measurements than Charlie will. This dynamic is captured by the uncertainty,

$$H(X|B) + H(Z|C) \geq q_{mu}, \tag{5.28}$$

where q_{mu} is a function of the overlap between the two measurements. A recent result that applies the triparite EUP in the presence of a quantum memory to CV is [92–94],

$$H(X|B) + H(Z|C) \geq \log 2\pi\hbar. \tag{5.29}$$

This result places a bound on the tripartite entropic quantity for CV observables. One area the entropic uncertainty principles have been applied is in QKD [17, 95] and QRNG [80, 96], for both CV and DV, to find device independent protocols by placing a bound on an eavesdropper's information using Alice and Bob's measurements.

5.3 Quantum Key Distribution

Quantum Key Distribution (QKD), BB84, was proposed in 1984 [14] as a solution to the key distribution problem. In this problem Alice wants to share a secret key with a remote party, Bob, but she only has public channels available to her that are potentially controlled by adversaries. The intended use of the key is for Bob to encrypt information and send it to Alice. This is currently solved by public key distribution protocols such as the RSA algorithm [84]. Older protocols like the RSA algorithm have security that relies on difficult to solve problems such as factorising large prime numbers or the discrete logarithm problem. It is expected that these problems will become easier to solve either due to the creation of quantum computers [97, 98] or perhaps advances in mathematics [99]. There is an effort to create post quantum computing public encryption and key distribution protocols [16] which is a study of classical algorithms that rely on problems that are difficult even for a quantum computer. The advantage of QKD over classical algorithms is that its security is guaranteed by physical principles [85].

5.3.1 BB84

In the BB84 protocol there are two remote parties, Alice and Bob linked together by an optical channel under the control of Eve. For the protocol to work Alice and Bob need to have access to an authenticated channel. The goal of Eve is to gain as much information from the channel as she can. If enough information is intercepted, Eve can deduce the final key distributed between Alice and Bob. An example of BB84 is given in Fig. 5.2. Alice starts the protocol by generating two random strings of n random bits, a_i and b_i. Bob will also start by generating a string of n random bits, b'_i. Alice will then encode the string a_i as either the horizontal vertical polarisation basis or the diagonal anti-diagonal basis of n photons determined by b_i. These two bases will be denoted by

$$\{|0\rangle, |1\rangle\} \qquad \text{and} \qquad \{|+\rangle, |-\rangle\}. \tag{5.30}$$

The diagonal anti-diagonal basis are given by,

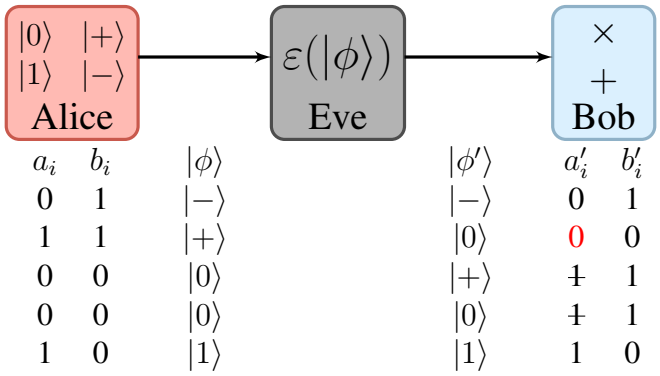
$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \qquad \text{and} \qquad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \tag{5.31}$$

When $b_i = 0$ then Alice will encode $a_i = 0$ as $|0\rangle$ or $a_i = 1$ as $|1\rangle$. If $b_i = 1$ then she will encode $a_i = 0$ as $|-\rangle$ and $a_i = 1$ as $|+\rangle$. These photons are sent to Bob through the channel controlled by Eve.

For each photon Bob receives he will measure the polarisation in the horizontal vertical basis if $b'_i = 0$ or the diagonal anti-diagonal basis if $b'_i = 1$. Bob stores all his measurements as a'_i. If Bob measures a photon in the same polarisation Alice used, assuming there is no channel noise, then $a_i = a'_i$. However as the two bases are not orthogonal if Bob uses the wrong basis then there is a 50% chance that $a_i \neq a'_i$. For Bob to correct his copy of a_i Alice publicly announces b_i on an authenticated channel and Bob will sift out any measurement where $b_i \neq b'_i$. Assuming there is no channel noise Alice and Bob will now share a string of secret bits.

One tactic Eve can take to learn a_i is to measure the polarisation of each photon as it passes by in a randomly selected basis. Using this measurement she can try to create a copy of the photon sent by Alice. Like Bob though her measurements will have a chance of an error. After the sifting step Alice will randomly select $n/2$ bits from the remaining a_i. Bob will compare this set of bits with his remaining a'_i. An attack from Eve as described above will result in a 25% error rate between a'_i and a_i. If the error rate threshold is achieved then Alice and Bob will abort the protocol. Eve can also use quantum mechanics to try improve her attack but she is limited by the no cloning theorem [82, 100]. If Alice and Bob decide to continue they will reconcile any errors between a_i

and a'_i using classical error correction protocols on the authenticated public channel.



a_i	b_i	$\|\phi\rangle$	$\|\phi'\rangle$	a'_i	b'_i
0	1	$\|-\rangle$	$\|-\rangle$	0	1
1	1	$\|+\rangle$	$\|0\rangle$	0	0
0	0	$\|0\rangle$	$\|+\rangle$	~~1~~	1
0	0	$\|0\rangle$	$\|0\rangle$	~~1~~	1
1	0	$\|1\rangle$	$\|1\rangle$	1	0

Figure 5.2: A example of the BB84 protocol. Alice generates two strings a_i and b_i and Bob b'_i. Using her strings Alice generates a series of states and sends them to Bob through a channel controlled by Eve, represented by the operation $\varepsilon(|\phi\rangle)$. Bob will measure the states from Alice in a basis determined by b'_i. Alice and Bob discard states that correspond with $b_i \neq b'_i$. By comparing a subset of a_i with a'_i they find an error rate of 33.3% and detect the presence of Eve.

Rather than discarding the secret when Eve is detected Alice and Bob can instead calculate how much information she may have intercepted. Alice and Bob can then use a one-way hashing function to disassociate the final key from Eve's information in a protocol step known as privacy amplification. The key rate, K, will be equal to the difference between the mutual information between Alice and Bob and Alice and Eve.

$$K = I(A:B) - I(A:E). \tag{5.32}$$

The mutual information between Alice and Eve can be calculated based on the type of attack Eve performed on the protocol. The key rate above is written for the case of direct reconciliation where Bob will correct his secret to match Alice. An alternative known as reverse reconciliation is for Alice to correct her secret to match Bob's. In situations such as high loss channels reverse reconciliation can yield a higher key rate [101]. With reverse reconciliation the key rate becomes,

$$K = I(A:B) - I(B:E). \tag{5.33}$$

5.3.2 CV QKD

CV QKD uses the quadrature modulations and measurements of phase and amplitude from a bright laser to distribute the shared secret [10, 15, 102]. The most popular of the CV QKD protocols is the family of Gaussian protocols [15]. Depending on the protocol

Alice will send Bob either a squeezed state randomly displaced in a quadrature randomly selected or a coherent state randomly displaced in both quadratures. To measure the received states Bob will use either a homodyne or a heterodyne measurement. There are in total four combinations of state preparation and measurement methods. For this thesis only the coherent state and squeezed state with homodyne detection protocol will be considered. This subsection is based on the work in Ref. [29] which contains a complete description and calculations of key rates for the Gaussian protocols.

For each of the Gaussian protocols there also exists an equivalent protocol that has a completely quantum description using an entanglement source. Rather than Alice encoding bits on in the quadratures of a laser she would use an entanglement source to generate the state. One mode from the entanglement source would be sent to Bob and the other would be measured by Alice in a basis selected by b_i. Alice's key is created using these measurements. From here Alice and Bob would follow the same protocol as in the prepare and measure case. This gives the family of Gaussian protocols sixteen possible protocols.

The optimal attack Eve can perform is a Gaussian collective attack [103, 104]. In this attack Eve entangles a state with each mode being sent to Bob. Each of the entangled states is stored in a quantum memory. After the protocol between Alice and Bob is complete, Eve can recall each state and perform an optimal measurement on the collective state to maximise her information based on the publicly exchanged information between Alice and Bob. The amount of information Eve can gather about Alice or Bob's collective state is limited by the Holevo bound which gives the key rate,

$$K^{\triangleright(\triangleleft)} \geq I(x_i : x_i') - \chi(x_i(x_i') : E). \tag{5.34}$$

The triangle signifies the direction of information flow with the right pointing triangle indicating direct reconciliation and the left pointing triangle reverse reconciliation. It is sufficient to prove security of the key exchange to consider Eve as always performing a Gaussian collective attack. This makes the security proof straightforward as the information quantities to calculate the key rate are a function of the first two moments of Alice and Bob's measurements as shown in the following sections for two of the Gaussian protocols.

Squeezed state with homodyne detection

This protocol is the most difficult to implement as a prepare and measure scheme as it needs squeezed coherent states. But it is the simplest as the entanglement scheme. In the prepare and measure scheme Alice will generate a strings of n random bits, b_i and a string of normally distributed numbers x_i sampled from a normal distribution $\mathbb{N}(0, V_A)$. Likewise Bob will generate a string of n random bits b_i'. Alice will then displace series of

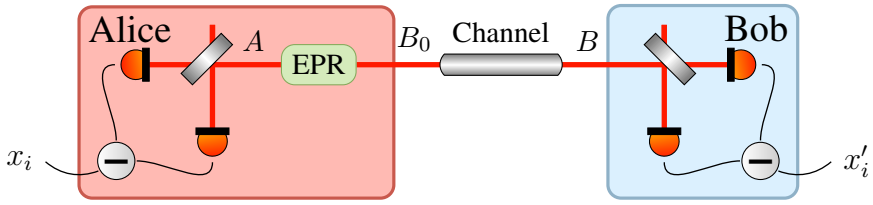


Figure 5.3: The squeezed state protocol with homodyne detection. Alice uses an EPR state to generate the modes A and B_0. Alice will measure A and sent B_0 to Bob through an uncontrolled channel. Bob will measure the transmitted state B with a homodyne detector.

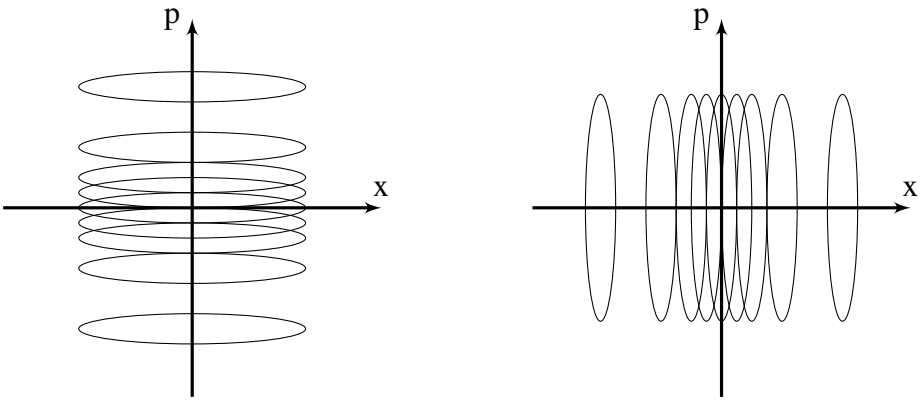


Figure 5.4: Alice randomly displaces a amplitude squeezed state by x_i in phase (a) when $b_i = 1$ or phase squeezed states in amplitude (b) when $b_i = 0$. The mixed state received by Bob is a thermal state of variance V.

states by x_i. These states are squeezed in phase and displaced in amplitude if $b_i = 0$ or squeezed in amplitude and displaced in phase if $b_i = 1$. The mode B is sent through an unsecure channel to get B'. Bob will then measure the received states with a homodyne detector in the phase quadrature when $b_i' = 1$ and the amplitude quadrature when $b_i' = 0$. The measurements are stored in the string x_i'. As in the BB84 protocol Alice will announce b_i and both Alice and Bob will discard any state measured using the wrong quadrature.

Consider each squeezed state generated by Alice with a squeezed quadrature variance of $1/V = e^{-r}$. The variance of x_i is chosen such that $V_A = V - 1/V$. The collective state sent by Alice when $b_i = 1$ can now be described by the covariance matrix,

$$\gamma = \begin{bmatrix} 1/V + V_A & 0 \\ 0 & V \end{bmatrix} = \begin{bmatrix} V & 0 \\ 0 & V \end{bmatrix}. \tag{5.35}$$

The same happens for $b_i = 0$. The states sent to Bob will collectively form a thermal state with a variance V where the displaced quadrature is indistinguishable from the squeezed quadrature. This is illustrated in Fig. 5.4.

In the entanglement equivalent protocol, shown in Fig. 5.3, Alice will measure one mode from an EPR source using a homodyne detector and similar to Bob she will switch the measurement quadrature based on b_i. Her measurements are recorded as x_i. By measuring A in a single quadrature the mode B' is projected into a squeezed state. The EPR state is described by the covariance matrix,

$$\gamma_{EPR} = \begin{bmatrix} V\mathbb{I} & \sqrt{V^2-1}\sigma_z \\ -\sqrt{V^2-1}\sigma_z & V\mathbb{I} \end{bmatrix}, \tag{5.36}$$

A collective attack from Eve can conveniently be modelled as a Gaussian loss channel. To calculate the mutual information between Alice and Bob and the Holevo bound for Alice (Bob) and Eve is now a simple task. The parameter ξ will be assigned to the channel to represent the Gaussian noise and T to represent the transmission. The channel can be applied to Eq. (5.36) using a CP-map on the second mode with $X = \sqrt{T}\mathbb{I}$ and $Y = (1 - T + T\xi)\mathbb{I}$ to give,

$$\gamma_{AB} = \begin{bmatrix} V\mathbb{I} & \sqrt{T(V^2-1)}\sigma_z \\ -\sqrt{T(V^2-1)}\sigma_z & (TV + 1 - T + T\xi)\mathbb{I} \end{bmatrix} \tag{5.37}$$

This covariance matrix gives a complete description of the state shared by Alice and Bob. From Eq. (5.37) the key rate can be found using the entropies for Gaussian distributions in Sec. 5.1.1 and Sec. 5.2.2. To simplify the following equations the noise relative to the input of the channel will be used and is given by,

$$\chi = \frac{1-T}{T} + \xi, \tag{5.38}$$

The mutual information between Alice and Bob can be found using Eq. (5.11). As the phase and amplitude quadrature are symmetric only one quadrature needs to be considered

$$I(x_i : x_i') = \frac{1}{2}\log\left[\frac{V+\chi}{\chi + 1/V}\right]. \tag{5.39}$$

The Holevo bound can be found by taking Eves state E to be the purifying state of Alice and Bob's joint state AB. For direct reconciliation the Holevo bound can be written as,

$$\chi(x_i : E) = \chi(x_i : B) = S(AB) - S(B|x_i). \tag{5.40}$$

Each term is calculated using Eq. (5.37) and Sec. 5.2.2. The value of $S(AB)$ is calculated

with Eq. (5.20) where the symplectic invariants are given by,

$$\Delta = V^2(1-2T) + 2T + T^2(V+\chi)^2 \tag{5.41}$$

$$D = T(V\chi + 1)^2. \tag{5.42}$$

The conditional entropy $S(B|x_i)$ is calculated again using Eq. (5.20) on Bob's projected state after Alice's measurement. The covariance for Alice's state is given by using Eq. (2.17). The projected state will have the symplectic eigenvalue of,

$$\lambda^2 = T^2(V+\chi)(\chi + 1/V). \tag{5.43}$$

For reverse reconciliation the Holevo bound is found by interchanging Alice and Bob to give,

$$\chi(x_i' : E) = \chi(x_i' : A) = S(AB) - S(A|x_i'). \tag{5.44}$$

The entropy $S(AB)$ is the same for both reconciliation directions and $S(A|x_i')$ is calculated in the same way as the direct reconciliation case. The symplectic eigenvalue of Alice's projected state is given by,

$$\lambda^2 = V\frac{V\chi + 1}{V+\chi} \tag{5.45}$$

Coherent states with homodyne detection

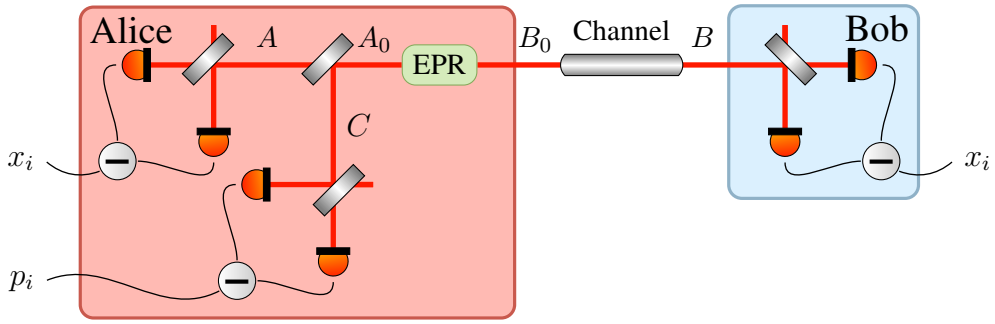


Figure 5.5: Entanglement based coherent state protocol with homodyne detection. Alice uses an EPR source to generate two entangled modes B_0 and A_0. She measures A_0 with a heterodyne and sends B_0 to Bob through an unsecured channel. Bob measures the mode B with a homodyne detector.

This protocol is the easiest to implement as a prepare and measure protocol and is commonly used for the study of CV QKD [105, 106]. This protocol is interesting as the prepare-and-measure (P&M) protocol does not require any other resource states other than vacuum. To start this protocol Alice will generate two strings of numbers x_i and

p_i from the distribution $\mathcal{N}(0, V_A)$ which she uses to create the state $|x_i + ip_i\rangle$. Bob again creates the string of random bits b'_i. Alice will send her states through the channel controlled by Eve and Bob will measure the received states in a quadrature determined by b'_i. After receiving all the state Bob will announce b'_i and Alice will discard either x_i or p_i depending on the quadrature measured by Bob. Bob on the other hand will keep all of his states.

Again the state measured by Bob will collectively appear as a thermal state as shown in Fig. 5.6. This time Alice sets the variance of her key to V_{A} and the collective state of B' will have a variance $V = V_{\mathrm{A}} + 1$

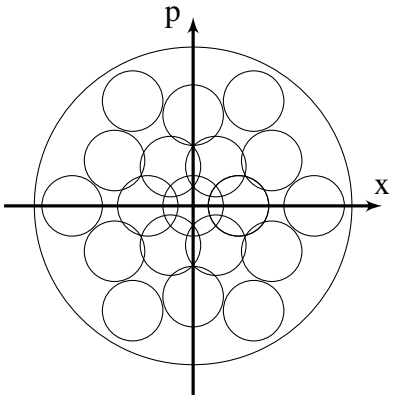


Figure 5.6: Alice randomly displaces a vacuum state to create the state $|x_i + ip_i\rangle$. The collective state of B_0 will be a thermal mixture of coherent states with state variance of V.

In the entanglement based scheme shown in Fig. 5.5 Alice will use a heterodyne to measure both quadratures simultaneously to get x_i and p_i. The initial state is described by Eq. (5.36) and after the channel by Eq. (5.37).

The keyrate for this protocol is calculated in a similar way to the squeezed state protocol but with the addition of one unit of shot noise to the variance of $\{x_i\}$ and $\{p_i\}$ from the hetrodyne measurement. The mutual information between Alice and Bob is now,

$$I(x_i : x'_i) = \frac{1}{2} \log \left[\frac{V + \chi}{\chi + 1} \right]. \tag{5.46}$$

As with the squeezed state protocol the Holevo bound can be found as it was in Eq. (5.40) except now there is an additional state, C, from Alice's heterodyne. The Holevo bound is now given by,

$$\chi(x_i : E) = S(AB) - S(BC|x_i). \tag{5.47}$$

The joint entropy $S(AB)$ is the same as the squeezed state protocol. Finding $S(BC : x_i)$ again requires the projection of the modes B and C after mode A has been measured

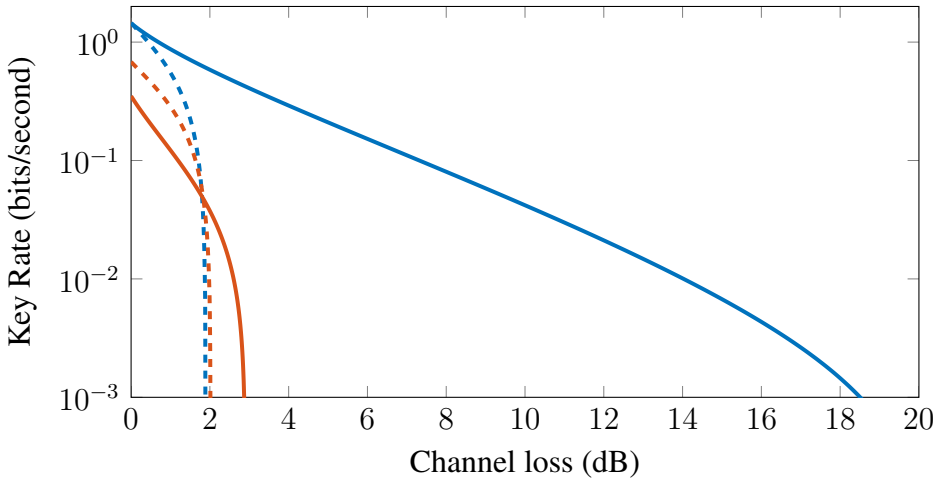


Figure 5.7: Comparison of the squeezed state protocol with homodyne detection (blue) against the coherent state protocol with homodyne detection (red) for both reverse reconciliation (solid) and direct reconciliation (dashed) with $\xi = 0.25$ and $V = 40$. The key rates are plotted again the channel loss T in the dB scale.

using Eq. (2.17). The joint state BCD is described by the covariance matrix,

$$\gamma^{BCD} = (S_{BS}^{AC_0} \otimes \mathbb{I}^B)\gamma^{ABC_0}(S_{BS}^{AC_0} \otimes \mathbb{I}^B)^T \tag{5.48}$$

With the symplectic invariants,

$$A = \frac{1}{V+1}[V + T(V+\chi)\det\gamma_{AB} + \Delta], \tag{5.49}$$

$$B = \frac{\sqrt{D}}{V+1}[T(V+\chi) + \sqrt{D}], \tag{5.50}$$

where Δ and $\det\gamma_{AB}$ are given in Eq. (5.42). The conditional entropy is then given by Eq. (5.20). For reverse reconciliation the conditional entropy $S(A|x_i')$ is the same as Eq. (5.45) for the squeezed state with homodyne detection protocol.

The squeezed state and heterodyne protocols discussed here are compared in Fig. 5.7 for both reverse and direct reconciliation protocols with $V = 40$ and $\xi = 0.25$ against channel loss in dB. The squeezed state protocol is the best performer of the protocols discussed here and it is shown to be one of the best of the Gaussian protocols for collective attacks in Ref. [29] for both direct and reverse reconciliation. The reverse reconciliation squeezed state with homodyne protocol performs much better in this example than all the other protocols. This is in contrast to long distance CV QKD demonstrations where the coherent state protocol with homodyne detection is used due to the ability to limit and control the amount of noise in the system [105, 107, 108].

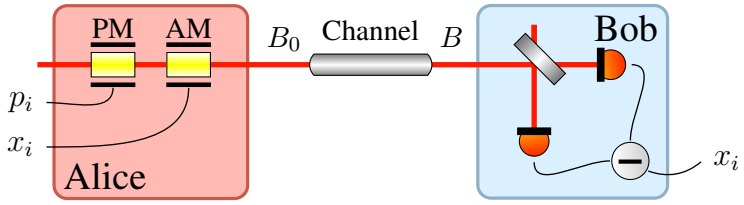


Figure 5.8: Prepare and measure coherent state protocol with homodyne measurement. This protocol is equivalent to the protocol in Fig. 5.5.

Finite size effects

The keyrates presented in Sec. 5.3.2 are only valid in the asymptotic regime. In a practical implementation of a QKD protocol there will be effects from the finite length of a key that could be exploited by Eve. These effects form a large part of the theory behind a practical implementation [107, 109]. Two of these effects, reconciliation efficiency and parameter estimation will be briefly explored here.

When Alice and Bob reconcile their secret key the error correction protocol will consume some information which reduces the overall mutual information between the two parties. How much information is consumed is represented by the reconciliation efficiency and is denoted by β. Accounting for β the key rate becomes,

$$K \geq \beta I(x_i : x_i') - \chi(x_i : E), \tag{5.51}$$

and similarly for the reverse reconciliation case. Using low density parity check codes β can be as high as 95% though the key rate has to be modified again to account for non-zero word error rates. Though as discussed in Ref. [110] the key rate is not formulated correctly to use LDPC codes. For a given transmission and noise of a channel the choice of reconciliation protocol can be chosen and optimized to maximize β [111].

As was found in Sec. 5.3.2 the key rate of a protocol can be characterised by three parameters, the EPR resource state variance, V, the transmission, T, and the channel noise, ξ. In a practical CV QKD protocol these parameters must be estimated from the measurements made by Alice and Bob to ensure the correct bound is found for the final secret key. To do this Alice or Bob must reveal m of the N measurements performed by Bob. The parameter estimation changes the key rate in two ways. The first is by Alice and Bob reducing the size of their final key by revealing measurements for parameter estimation. The second is the uncertainty of the estimation of the two parameters. The uncertainty in the estimation is captured by the probability of failure as set by the parameter ϵ_{PE}. The key rate can be rewritten to include the effect of parameter estimation with $\frac{m}{N}$ for the

reduction in the key and ϵ_{PE} [109],

$$K = \frac{m}{N}[\beta I(x:y) - S_{\epsilon_{PE}}(y:E)], \tag{5.52}$$

where $S_{\epsilon_{PE}}(y:E)$ is calculated from the worst case estimates of our channel parameters. The value of m and V and can optimised in order to maximize the key for a given channel. There are a number of other finite key effects that contribute to the security proof of a QKD protocol to show that it is secure with respect to ϵ, where ϵ is the probability that the protocol failed to produce a secret key. The ultimate goal for studying finite key effects is to produce a composable security proof [112, 113] that allows the protocol to be interoperable with other cryptographic systems.

Chapter 6

Method of Moments Channel Noise Estimator

6.1 Introduction

One of the major tasks for CV QKD introduced in Sec. 5.3 is channel parameter estimation. In this chapter two new estimators for the channel noise are introduced based on the method of moments. The method of moments uses the moments of data being used to estimate parameters. The new estimators have the advantage of being able to use the whole shared secret between Alice and Bob including those kept secret from Eve. The proposed estimator has a lower variance for high-loss channels than the maximum likelihood estimator that has been previously used. The work in this chapter is published in Ref. [88]

This chapter is organised as follows. Sec. 6.2 will review some previously proposed channel noise estimators and introduce modelling the channel as an additive Gaussian noise channel. Sec. 6.3 will detail the method of moments and its application to CV QKD. This section proposes two channel noise estimators based on the method of moments. These estimators are shown to be asymptotically unbiased and their performance is compared against two previous estimators in Sec. 6.4. Sec. 6.5 will conclude the chapter with an investigation into the effect of the two new estimators have on the keyrate of the coherent state with homodyne protocol. The hat decoration, $\hat{}$, for this chapter denotes an estimator rather than a operator.

6.2 Channel Model

In ref. [109] the authors propose a method of estimating the two channel parameters by modelling the protocol using as classical loss channel with additive Gaussian noise:

$$y_i = tx_i + z_i \qquad i = 1, 2, \ldots N. \tag{6.1}$$

Here x_i is the data sent by Alice, y_i is Bob's measurement data, z_i is a Gaussian noise term with variance $\sigma^2 = 1 + T\xi$ and mean 0 and $t = \sqrt{T}$. To estimate the channel parameters, t and σ Alice and Bob reveal a subset of $m < N$ measurements. The channel model Eq. (6.1) is well studied and has the maximum likelihood estimators [109]:

$$\hat{t} = \frac{\sum_{i=1}^{m} x_i y_i}{\sum_{i=1}^{m} x_i^2} \quad \text{and} \quad \hat{\sigma}^2_{\text{MLE}} = \frac{1}{m}\sum_{i=1}^{m}\left(y_i - \hat{t}x_i\right)^2, \tag{6.2}$$

with their distributions given by,

$$\hat{t} \sim \mathcal{N}\left(t, \frac{\sigma^2}{\sum_{i=1}^{m} x_i^2}\right) \quad \text{and} \quad \frac{m\hat{\sigma}^2_{\text{MLE}}}{\sigma^2} \sim \chi^2(m-1). \tag{6.3}$$

Here $\mathcal{N}$ denotes a normal distribution and χ^2 is the chi-squared distribution. The estimators, Eq. (6.2) are then used to find the worst case for t and σ^2 as described in [109]. That is the minimum of t and the maximum of σ^2 with in the confidence interval $1 - \epsilon_{\text{PE}}$. The parameter ϵ_{PE} is the probability that the parameter estimation failed (Typically $\epsilon_{\text{PE}} = 10^{-10}$). Using the theoretical distributions given in Eq. (6.3) the worst case estimators are given by,

$$t_{\min} \approx \hat{t} - z_{\epsilon_{\text{PE}}/2}\text{SD}(\hat{t}), \tag{6.4}$$

$$\sigma^2_{\max} \approx \hat{\sigma}^2_{\text{MLE}} + z_{\epsilon_{\text{PE}}/2}\text{SD}(\hat{\sigma}^2_{\text{MLE}}) \tag{6.5}$$

Here SD is the standard deviation function and $z_{\epsilon_{\text{PE}}/2} = \text{erf}^{-1}(1 - \epsilon_{\text{PE}}/2)$ where erf(x) is the error function. Equation (5.37) can be rewritten for the worst case noise and transmission,

$$\Gamma_{\epsilon_{\text{PE}}} = \begin{pmatrix} (V_{\text{A}} + 1)\,\mathbb{I}_2 & t_{\min}\sqrt{V_{\text{A}}^2 + 2V_{\text{A}}}\sigma_z \\ t_{\min}\sqrt{V_{\text{A}}^2 + 2V_{\text{A}}}\sigma_z & (t^2_{\min}V_{\text{A}} + \sigma^2_{\max})\,\mathbb{I}_2 \end{pmatrix}. \tag{6.6}$$

Another proposed estimator from Ref. [114] uses a second modulation transmitted with the key to assist the estimation of the channel parameters. This assumes the second modulation will experience the same channel as the modulation used for the final key. For the protocol analyzed in their paper, Alice sends Bob squeezed displaced vacuum states with a squeezed quadrature variance of V_{S}. By setting $V_{\text{S}} = 1$ the protocol becomes the coherent state protocol. The parameters estimated are the channel transmission T and the excess noise relative to the output $V_\xi = T\xi$. Thanks to the second modulation this

estimator is able to use N states for the key and parameter estimation,

$$\hat{T} = \frac{\left(\sum_{i=1}^{N} x_{\mathrm{M2},i} y_i\right)^2}{\left(N V_{\mathrm{M2}}\right)^2}, \tag{6.7}$$

$$\hat{V}_\xi = \frac{1}{N}\sum_{i=1}^{N}\left(y_i - \sqrt{\hat{T}} x_{\mathrm{M2},i}\right)^2 - \hat{T} V_{\mathrm{A}} - 1, \tag{6.8}$$

where $x_{\mathrm{M2},i}$ is the displacement of the second modulation from Alice. These estimators were shown to be asymptotically unbiased and to have the variances:

$$\mathrm{Var}(\hat{T}) = \frac{4}{N} T^2 \left(2 + \frac{V_{\mathrm{N}}}{T V_{\mathrm{M2}}}\right), \tag{6.9}$$

$$\mathrm{Var}(\hat{V}_\xi) = \frac{2}{N} V_N^2 + V_{\mathrm{A}}^2 \mathrm{Var}(\hat{T}), \tag{6.10}$$

where $V_{\mathrm{N}} = 1 + V_\xi + T V_{\mathrm{A}}$ and V_{M2} is the variance of the second modulation. The authors then suggests using the linear combination in Eq. (6.11) to find the optimal estimator T^{opt} and V_ξ^{opt} at a high channel transmission.

$$\hat{\theta}_{\mathrm{opt}} = \alpha \hat{\theta}_1 + (1-\alpha)\hat{\theta}_2, \tag{6.11}$$

where $\hat{\theta}_1$ and $\hat{\theta}_2$ are two different estimators for either V_ξ or T. The optimum value of α to achieve a minimum variance from two estimators with a covariance of 0 is given by,

$$\alpha = \frac{\mathrm{Var}(\hat{\theta}_2)}{\mathrm{Var}(\hat{\theta}_1) + \mathrm{Var}(\hat{\theta}_2)}. \tag{6.12}$$

This can be found by minimising $\mathrm{Var}(\hat{\theta}_{opt})$ with respect to α. A derivation of α is shown in App. D.3. The variance of $\hat{\theta}_{\mathrm{opt}}$ is then given by,

$$\mathrm{Var}(\hat{\theta}_{\mathrm{opt}}) = \frac{\mathrm{Var}(\hat{\theta}_1)\mathrm{Var}(\hat{\theta}_2)}{\mathrm{Var}(\hat{\theta}_1) + \mathrm{Var}(\hat{\theta}_2)}. \tag{6.13}$$

By construction $\hat{\theta}_{\mathrm{opt}}$ will have a variance less than or equal to the variance of the estimators $\hat{\theta}_1$ and $\hat{\theta}_2$. The linear combination will also preserve the bias properties of the two estimators.

6.3 Theory

The estimators in Eq. (6.2) are found by maximizing the log likelihood joint probability distribution $\ln p(x_i, y_i; \sigma^2, t, V_A)$. An alternative is to use the method of moments (MM) [115] to find the estimators. The method of moments is a simple way to find an estimator but it has no optimality properties. It performs best with a long data record which makes it suitable to CV QKD as typically the data record is $> 10^8$ [106]. Consider the distribution of Bob's measurements which can be described by the normal distribution $\mathcal{N}(0, t^2 V_\mathrm{A} + \sigma^2)$. The moments of this distribution can then be solved as a system of equations to find the method of moments estimators. As Bob's data is normally distributed around 0 the first moment will be zero and the second moment is given by the variance,

$$\sigma_\mathrm{B}^2 = t^2 V_\mathrm{A} + \sigma^2. \tag{6.14}$$

All other moments for this distribution will be a function of σ_B^2 giving only one independent non zero moment. This method will only provide one estimator so a decision must be made between t and σ^2.

The goal of parameter estimation for QKD is to maximize the keyrate for long distances. The limiting factor for protocols with a high loss channel is the excess noise [102]. For this reason Eq. (6.14) will be used to find a better estimator for the output noise. Starting with Eq. (6.14) and substituting the estimator for t and the sample variance for σ_B the initial estimator for the noise relative to the output is given by,

$$\hat{\sigma}_\mathrm{mm}^2 = \hat{\sigma}_\mathrm{B}^2 - \hat{t}^2 V_\mathrm{A}, \tag{6.15}$$

where $\hat{\sigma}_\mathrm{B}^2$ is given by the sample variance $\frac{1}{N}\sum y_i^2$. To use this estimator Alice and Bob can publicly reveal V_A and σ_B^2 without giving away any more of the shared secret to Eve [109]. It was found that by treating V_A as an unknown parameter and using the estimate $\hat{\sigma}_\mathrm{A}^2 = \frac{1}{N}\sum x_i^2$ in its place the variance of the MM estimator decreased. The variances of $\hat{\sigma}_\mathrm{mm}^2$ and the new estimator $\hat{\sigma}_\mathrm{MM}^2$ are compared in appendix App. D.1. This improvement comes from increasing the covariance between σ_B^2 and $t^2\sigma_\mathrm{A}^2$ and is demonstrated by the following property of variance,

$$\mathrm{Var}(\sigma_\mathrm{B}^2 - t^2\sigma_\mathrm{A}^2) = \mathrm{Var}(\sigma_\mathrm{B}^2) + \mathrm{Var}(t^2\sigma_\mathrm{A}^2) - 2\mathrm{Cov}(\sigma_\mathrm{B}^2, t^2\sigma_\mathrm{A}^2). \tag{6.16}$$

Substituting $\hat{\sigma}_\mathrm{A}$ the final MM estimator is given by,

$$\hat{\sigma}_\mathrm{MM}^2 = \hat{\sigma}_B^2 - \hat{t}^2\hat{\sigma}_A^2. \tag{6.17}$$

The improvement in the variance of the estimator $\hat{\sigma}^2_{\mathrm{MM}}$ over $\hat{\sigma}^2_{\mathrm{MLE}}$ can be seen in Fig. 6.1 as the transmission approaches zero for a fixed value of V_{A} and m. The variance of these estimators where $t = 0$ are given by

$$\mathrm{Var}(\hat{\sigma}^2_{\mathrm{MM}}) = \frac{2\sigma_B^4}{N} \tag{6.18}$$

$$\mathrm{Var}(\hat{\sigma}^2_{\mathrm{MLE}}) = \frac{2\sigma_B^4}{m} \tag{6.19}$$

When the two are compared $\mathrm{Var}(\hat{\sigma}^2_{\mathrm{MM}})$ is found to be better by a factor of $\frac{m}{N}$.

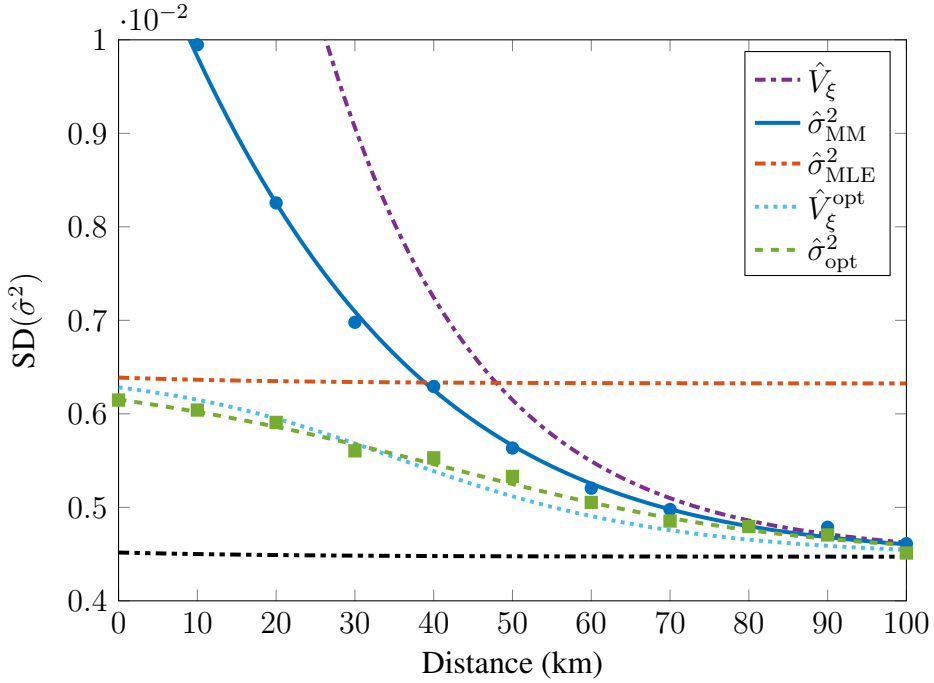


Figure 6.1: Plot of the standard deviation of the different noise estimators vs distance in a fiber channel with a loss of 0.2dB/km: $\hat{V}_\xi$ (dot dashed), $\hat{\sigma}^2_{\mathrm{MM}}$ (solid), $\hat{\sigma}^2_{\mathrm{MLE}}$ (dot dot dashed), $\hat{V}^{\mathrm{opt}}_\xi$ (dotted) and $\hat{\sigma}^2_{\mathrm{opt}}$ (dashed). A stochastic simulation of the coherent state protocol was repeated 5000 times to obtain the data points for $\hat{\sigma}^2_{\mathrm{MM}}$ (circles) and $\hat{\sigma}^2_{\mathrm{opt}}$ (squares). The parameters used were $V_A = 3$, $\xi = 0.01$, $m = 0.5{\times}10^5$, $N = 10^5$ and $V_2 = 10$. The black dash dot dot line is the standard deviation of the MLE with $m = N$ and represents the best estimate Alice and Bob can make of the channel noise using the MLE. The MM estimators and the double modulation estimators approach this standard deviation as the channel losses increases.

Interestingly $\hat{\sigma}^2_{\mathrm{MM}} = \hat{\sigma}^2_{\mathrm{MLE}}$ when both estimators are used on the N transmitted states. Such is the case at the range limit of a protocol, where for a positive key rate almost all of the states need to be revealed for parameter estimation. Using Eq. (6.2) on the N

transmitted states gives,

$$\hat{\sigma}^2_{\mathrm{MLE}} = \frac{1}{N}\sum_{i=1}^{N}(y_i - \hat{t}x_i)^2 \tag{6.20}$$

$$= \frac{1}{N}\sum_{i=1}^{N} y_i^2 - \frac{1}{N}\frac{\left(\sum_{i=1}^{N} x_i y_i\right)^2}{\sum_{i=1}^{N} x_i^2} \tag{6.21}$$

$$= \hat{\sigma}^2_{\mathrm{B}} - \hat{t}^2\hat{\sigma}^2_{\mathrm{A}} \tag{6.22}$$

$$= \hat{\sigma}^2_{\mathrm{MM}}. \tag{6.23}$$

With this result it can be shown that $\hat{\sigma}^2_{\mathrm{MM}}$ from Eq. (6.17) is a combination of two estimators. By ordering the exchanged states into the publicly revealed m subset and the secret $n = N - m$ subset to find

$$\hat{\sigma}^2_{\mathrm{MM}} = \frac{1}{N}\left(\sum_{i=1}^{m} y_i^2 + \sum_{i=m+1}^{N} y_i^2 + \hat{t}^2\left(\sum_{i=1}^{m} x_i^2 + \sum_{i=m+1}^{N} x_i^2\right)\right) \tag{6.24}$$

$$= \frac{1}{N}\sum_{i=1}^{m}(y_i - \hat{t}x_i)^2 + \frac{1}{N}\left(\sum_{i=m+1}^{N} y_i^2 - \hat{t}^2\sum_{i=m+1}^{N} x_i^2\right) \tag{6.25}$$

$$= \frac{1}{N}(m\hat{\sigma}^2_{\mathrm{MLE}} + n\hat{\sigma}^2_{\mathrm{MM}''}), \tag{6.26}$$

where $\hat{\sigma}^2_{\mathrm{MM}''}$ is the MM estimator applied to n states and $\hat{\sigma}^2_{\mathrm{MLE}}$ and $\hat{t}$ applied to m states. This leads to the next estimator presented in the chapter. As in Ref. [114] an optimum linear combination of two estimators can be found using Eq. (6.11) provided the two estimators have a covariance of 0. This is the case for $\hat{\sigma}^2_{\mathrm{MLE}}$ and $\hat{\sigma}^2_{\mathrm{MM}''}$ given $\hat{t}$ and $\hat{\sigma}^2_{\mathrm{MLE}}$ are independent [116]. A full derivation is given in App. D.3. The optimum estimate of the noise estimator is given by,

$$\hat{\sigma}^2_{\mathrm{opt}} = \alpha\hat{\sigma}^2_{\mathrm{MLE}} + (1-\alpha)\hat{\sigma}^2_{\mathrm{MM}''}. \tag{6.27}$$

Here α is given in Eq. (6.12).

6.4 Performance

For the purposes of CV QKD, it is important to consider the variance and the bias of the parameter estimators. Finding an unbiased estimator with a minimized variance will ultimately lead to an increase in the key rate and secure distance of the protocol.

For the MM estimators, the variance and mean are difficult to find due to the division

operation required for $\hat{t}$. For this chapter a standard method in uncertainty analysis is used where the variance is approximated from a first order Taylor series expansion [115]. Given an estimator $\hat{\theta}$ that is some function of $\boldsymbol{J} = \{J_1(\boldsymbol{y}), J_2(\boldsymbol{y}), \ldots, J_r(\boldsymbol{y})\}$, where $J_i(\boldsymbol{y})$ is some statistic from the data vector $\boldsymbol{y}$, the variance is approximated by,

$$\mathrm{Var}(\hat{\theta}(\mathbf{J})) \approx \left.\frac{\partial \hat{\theta}}{\partial \mathbf{J}}\right|_{\mathbf{J}=\boldsymbol{\mu}}^{T} \boldsymbol{C}_J \left.\frac{\partial \hat{\theta}}{\partial \mathbf{J}}\right|_{\mathbf{J}=\boldsymbol{\mu}} \tag{6.28}$$

and the mean by

$$E(\hat{\theta}(\mathbf{J})) \approx \hat{\theta}(\boldsymbol{\mu}). \tag{6.29}$$

Here $\boldsymbol{\mu}$ is the expected value of our statistics $\boldsymbol{J}$ and $\boldsymbol{C}_J$ is the covariance matrix for $\boldsymbol{J}$. This method assumes that the statistics $\boldsymbol{J}$ will have a low variance and the estimator $\hat{\theta}$ will be roughly linear around $\boldsymbol{\mu}$. That is Eq. (6.28) and Eq. (6.29) will be the asymptotic variance and mean. To apply this method the estimators are rewritten in terms of the data statistics, $\hat{\sigma}^2_{\mathrm{B}}$, $\hat{\sigma}^2_{\mathrm{A}}$, $\hat{\sigma}_{\mathrm{A'B'}}$ and $\hat{\sigma}^2_{\mathrm{A'}}$. Here $\hat{\sigma}_{\mathrm{A'B'}}$ is the sample covariance. Here A' and B' are used to indicate the statistic was estimated from the m subset of states used for parameter estimation. The estimator $\hat{\sigma}^2_{\mathrm{MM}}$ becomes,

$$\hat{\sigma}^2_{\mathrm{MM}} = \hat{\sigma}^2_{\mathrm{B}} - \left(\frac{\hat{\sigma}_{\mathrm{A'B'}}}{\hat{\sigma}^2_{\mathrm{A'}}}\right)^2 \hat{\sigma}^2_{\mathrm{A}}, \tag{6.30}$$

where $\hat{t} = \hat{\sigma}_{\mathrm{A'B'}}/\hat{\sigma}^2_{\mathrm{A'}}$. The matrix $\boldsymbol{C}_J$ can be found using the variance of the sample variance and the properties of the covariance and variance functions. The elements of $\boldsymbol{C}_J$ are given in App. D.2.1. Applying Eq. (6.28) the variance is given by

$$\mathrm{Var}(\hat{\sigma}^2_{\mathrm{MM}}) \approx \frac{2\sigma^4}{N} + \left(\frac{1}{m} - \frac{1}{N}\right) 4t^2\sigma^2 V_A. \tag{6.31}$$

The final variance in Eq. (6.31) was achieved by making the substitution,

$$E[\hat{\sigma}^2_{\mathrm{A}}] = E[\hat{\sigma}^2_{\mathrm{A'}}] = V_{\mathrm{A}}, \quad E[\frac{\hat{\sigma}_{\mathrm{A'B'}}}{\hat{\sigma}^2_{\mathrm{A'}}}] = t \quad \text{and} \quad E[\hat{\sigma}^2_{\mathrm{B}}] = t^2 V_{\mathrm{A}} + \sigma^2. \tag{6.32}$$

For the estimator $\hat{\sigma}^2_{\mathrm{MM}''}$ a similar equation was found,

$$\mathrm{Var}(\hat{\sigma}^2_{\mathrm{MM}''}) \approx \frac{2\sigma^4}{n} + \left(\frac{1}{m} + \frac{1}{\sigma^2 n}\right) 4t^2\sigma^2 V_A. \tag{6.33}$$

As $\hat{\sigma}^2_{\mathrm{MM}''}$ uses different statistics $\boldsymbol{C}_J$ will be different. This is given in App. D.2.2. The

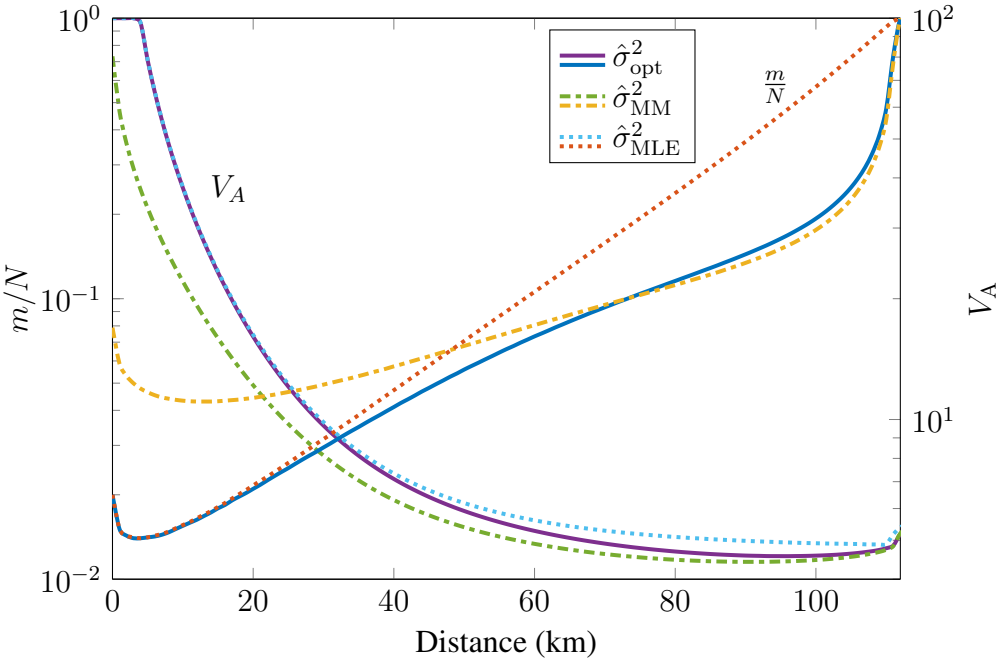


Figure 6.2: The optimized values of $\frac{m}{N}$ and V_{A} for the key rates in Fig. 6.3 where $N = 10^9$ using $\hat{\sigma}^2_{\text{MLE}}$ (dotted), $\hat{\sigma}^2_{\text{MM}}$ (dot dashed) and $\hat{\sigma}^2_{\text{opt}}$ (solid) to estimate the excess noise. Beyond 40 km more states are able to be used in the final key when the optimal or the MM estimator is used.

variance of the optimal estimator is given by [114]

$$\text{Var}(\hat{\sigma}^2_{\text{opt}}) = \frac{\text{Var}(\hat{\sigma}^2_{\text{MLE}})\text{Var}(\hat{\sigma}^2_{\text{MM}''})}{\text{Var}(\hat{\sigma}^2_{\text{MLE}}) + \text{Var}(\hat{\sigma}^2_{\text{MM}''})}. \tag{6.34}$$

The standard deviation of the estimators $\hat{\sigma}^2_{\text{MM}}$ and $\hat{\sigma}^2_{\text{opt}}$ are plotted as a function of the channel distance in Fig. 6.1. Using Eq. (6.29) shows the estimator, $\hat{\sigma}^2_{\text{MM}}$ is asymptotically unbiased. A series of 5000 stochastic simulations of the coherent state protocol using $N = 10^5$. The variance of the estimators from this simulations are shown in Fig. 6.1 and have a good agreement with Eq. (6.31) and Eq. (6.34). In practical demonstrations N has been of the order 10^8 to 10^9 [106].

6.5 Discussion & Conclusion

This chapter investigated using the method of moments to estimate the noise in a linear channel relative to the output for a QKD protocol. The MM estimator allows for Alice and Bob to use better estimates of the variances from the complete shared secret. Using these variances allows the proposed estimators in this chapter to approach the performance of the MLE used on the entire shared secret for a high loss channel.

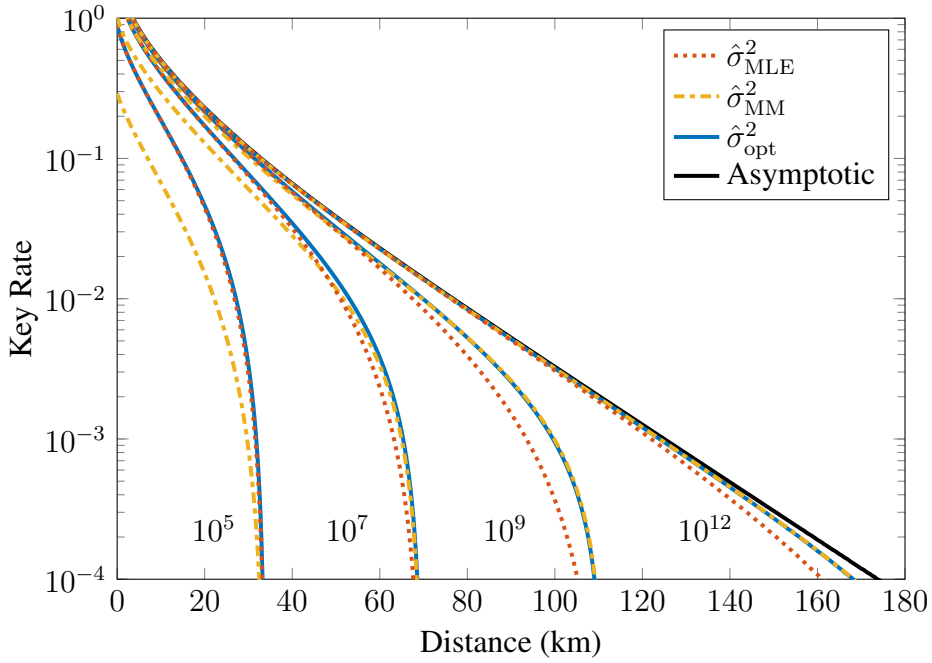


Figure 6.3: Plot of key rate with finite key effects relating to parameter estimation. The values V_{A} and m have been optimized with $\xi = 0.01$ and $\beta = 0.95$ to maximize key rate using $\hat{\sigma}^2_{\mathrm{MLE}}$ (dotted), $\hat{\sigma}^2_{\mathrm{MM}}$ (dot dashed) and $\hat{\sigma}^2_{\mathrm{opt}}$ (solid) to estimate the excess noise for (from left to right) $N = 10^5$, $N = 10^7$, $N = 10^9$ and $N = 10^{12}$. The asymptotic key rate with V_{A} optimized is also plotted (black solid). As expected the maximum distance increases with the size of N. The optimal estimator outperforms the MLE and MM estimator. As with Fig. 6.1 it was found the MM estimator is worse than the MLE at low channel loss but is better with a lossy channel.

To simplify our analysis it was assumed that both Alice's modulation and the channel noise are Gaussian with a mean of zero. These assumptions are necessary for finding the variance of the $\hat{\sigma}^2_{\mathrm{MM}}$ and $\hat{\sigma}^2_{\mathrm{MLE}}$. The MM estimators do not require the Gaussian assumption as they are estimating the second moment. It is possible that Eve could find a non Gaussian state that could cause Alice and Bob to underestimate Eves influence on the channel using the method to find the keyrate discussed in this chapter. Which state Eve would need to do this is not investigated in this chapter.

In a situation where the added noise is non Gaussian, Alice and Bob should not use the Gaussian approximation for estimating the variance of their estimators. Instead, they should use the general formula for estimating the distribution of the estimators, for example, when N is large, $\mathrm{Var}(\hat{\sigma}^2_{\mathrm{B}})$ in App. D.2.1 should be replaced by $\mathrm{Var}(\hat{\sigma}^2_B) = \mu_4/M - \mu_2^2/M$ where μ_k is the k-th moment of Bob's measurements [117].

When compared with other estimation methods in Fig. 6.1, it was found that the method of moments based estimators are comparable in performance to the method proposed in ref. [114] without requiring extra modulations and an improved performance

over the MLE for high loss channels. The result of the improvement in the key rate can be observed in Fig. 6.3 where the MM estimator based key rate is higher than when the MLE is used and the optimum estimator always produces the best keyrate. It is interesting to note that the estimators discussed in this chapter will never increase the maximum distance for a QKD protocol. The reason for this is shown in Fig. 6.2 where the maximum transmission distance the optimal m is N and the MLE and MM estimators are equal.

After reconciliation Alice and Bob are able to estimate the key rate bound again but this time with all N measurements [113]. Doing this will give an improved key rate. For high loss channels this improvement will be mostly due to the improved estimate of the covariance matrix. The MM estimators could be used to determine a rough key rate before the protocol commits to performing the reconciliation step.

With the simplicity of the method of moments, this estimator can also be modified to be used with other CV QKD protocols such as the four state protocol [102] or to include more protocol parameters [107].

Chapter 7

One Side Device Independent CV QKD with EPR states

7.1 Introduction

The physically guaranteed security with minimal additional assumptions from QKD has crystallised into two fronts. In the first place a lower bound on the extractable secret key length is desired that accounts for an arbitrarily powerful Eve [118–121]. The second, as briefly explored in Sec. 5.3 and Ch. 6, to close any gaps that may exist between a theoretical QKD protocol and its practical realisation. Essentially, this is the problem of whether or not the honest parties (Alice and Bob) have correctly characterised their experimental devices. These gaps can be closed one by one as various loopholes, due to miss-characterised devices, are pointed out [122–125]. However it is possible to rigorously surmount all side-channel attacks by harnessing non-local quantum correlations [18, 92, 126]. A fully device independent protocol is possible using a loophole free Bell test. As discussed in Ch. 4 a true loophole free Bell test using CV is difficult to achieve. A compromise is one-side-device-independent (1sDI) protocol where only the devices controlled by Bob or Alice are trusted. It is this problem tackled in this chapter for the entire Gaussian family of CV-QKD protocols. In this chapter six protocols are identified that can be proven secure in a 1sDI setting. The new security proofs are accompanied by proof-of principle experimental demonstrations of the most basic of the EPR based protocols, squeezed state protocol with homodyne detection, and a prepare and measure coherent state protocol. The work in this chapter is published in ref. [17].

This chapter is organised as follows. Sec. 7.2 will detail the application of the tripartite entropy uncertainty to the Gaussian family of CV QKD protocols. The experimental details for the demonstration of these protocols is presented in Sec. 7.3 with some experimental modelling. The results are presented in Sec. 7.4 with a conclusion in Sec. 7.5.

7.2 Theory

This section will derive the key rate in a slightly different way to what appeared in Ref. [17] to account for reconciliation efficiency. This key rate is the one used for the presented experimental results. The family of Gaussian CV QKD protocols were introduced in Sec. 5.3 along with a brief derivation of the secret key rate against collective attacks. In this section a new key rate is derived for the squeezed state with homodyne protocol using the EUP in Eq. (5.29),

$$H(X_{\mathrm{A}}|E) + H(P_{\mathrm{A}}|B) \geq \log 2\pi\hbar, \tag{7.1}$$

where X_{A} and P_{A} are quadrature measurements made by Alice and E and B represent the unmeasured state of Eve and Bob. Consider the reverse reconciliation key rate from Eq. (5.51),

$$K^{\triangleleft} = \beta I(X_{\mathrm{A}} : X_{\mathrm{B}}) - \chi(X_{\mathrm{B}} : E), \tag{7.2}$$

where β is the reconciliation efficiency. Recalling that,

$$S(X_{\mathrm{B}}|E) = H(X_{\mathrm{B}}) + \int p(X_{\mathrm{B}}) S(\rho_{\mathrm{E}}^{X_{\mathrm{B}}}) \mathrm{d}x, \tag{7.3}$$

the Holevo bound can be rewritten in terms of conditional entropy.

$$\chi(X_{\mathrm{B}} : E) \leq H(X_{\mathrm{B}}) - S(X_{\mathrm{B}}|E). \tag{7.4}$$

As in Sec. 5.3.2 Eve is considered the purifying state of Alice and Bob's joint state that is $S(P_{\mathrm{B}}|E) \leq H(P_{\mathrm{B}}|P_{\mathrm{A}})$. The Holevo bound can again be rewritten with the uncertainty Eq. (5.29) to be,

$$\chi(X_{\mathrm{B}} : E) \leq H(X_{\mathrm{B}}) + H(P_{\mathrm{B}}|P_{\mathrm{A}}) - \log 4\pi \tag{7.5}$$

Using Eve's optimal attack which is known to be a Gaussian collective attack the Shannon entropies for Gaussian states given in Sec. 5.1.1 can be used to find the final reverse reconciliation key rate as,

$$K^{\triangleleft} \geq \beta I(X_{\mathrm{B}} : X_{\mathrm{A}}) + \log 4\pi - H(P_{\mathrm{B}}|P_{\mathrm{A}}) - H(B) \tag{7.6}$$

$$= \beta \log \sqrt{\frac{V_{\mathrm{B}}^{X}}{V_{\mathrm{B|A}}^{X}}} - \log \sqrt{\frac{4\pi}{e^2 V_{\mathrm{B|A}}^{P} V_{\mathrm{B}}^{X}}}. \tag{7.7}$$

Here V_i^j represents the variance of the measurement by party $i = \{\mathrm{A}, \mathrm{B}\}$ of the quadrature $j = \{X, P\}$. Similarly $V_{i|i'}^{j}$ is the variance of party i conditioned on the results of i'.

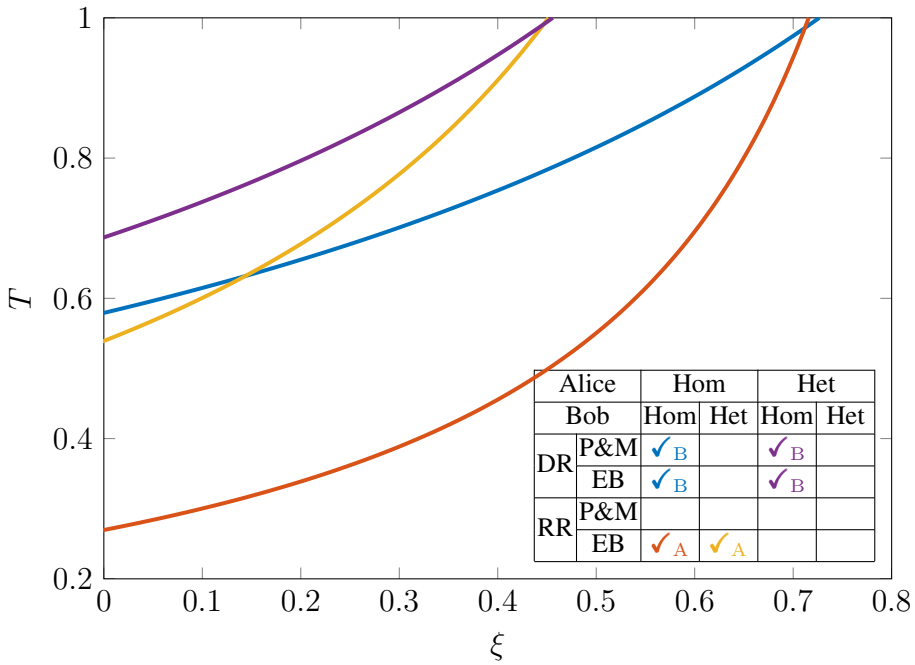


Figure 7.1: Secure regions for 1sDI CV QKD protocols for a Gaussian channel parameterised by transmission T and excess noise ξ. DR protocols are plotted in blue when Alice homodynes and purple when Alice heterodynes. RR schemes are plotted in red when Bob homodynes and yellow when Bob heterodynes. For each protocol, secure communication is possible for all channels above the corresponding line. Inset: summary of 1sDI CV QKD protocols where subscript A (B) indicates the security is independent of Alice's (Bob's) devices.

The key rate for the direct reconciliation case is made by permuting the labels, A and B. Eq. (7.7) was also calculated in Ref. [92] but the proof was incomplete as it relied on the assumption of the applicability of the entropic uncertainty relation. Moreover, it was incorrectly concluded that this method would never predict a positive key when applied to coherent state or heterodyne protocols. In fact the extension of Eq. (7.7) to the other Gaussian protocols is straightforward and is given in Ref. [17].

7.2.1 1sDI CV QKD

For 1sDI QKD protocols only Alice or Bob needs to be trusted with a assumed set of quantum operations while the other is untrusted and considered a black box. A conceptual picture of this is given in Fig. 7.2. The 1sDI nature of Eq. (7.7) comes from its dependence on measuring a known observable on only one side. For example only Bob is required to measure the amplitude or phase quadrature to apply the EUR. Although we write the expression as $V^X_{\mathrm{A|B}}$ Alice could be making any measurement and the key rate Eq. (7.7) would still hold. That is Eq. (7.7) is independent from Alice for reverse reconciliation and

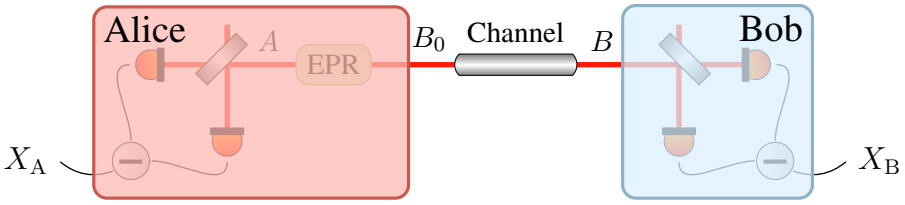


Figure 7.2: Conceptual picture of a 1sDI CV QKD protocol. From the perspective of Alice (Bob) the local devices are known and allow a secret key to be extracted from a direct (reverse) reconciliation protocol, even though the other party exists only as an unknown blue (red) box.

from Bob for direct reconciliation. For the device independence to hold two assumptions are made: the stations are secure and the measurements are causally independent [127, 128].

Thus for EPR based protocols with homodyne measurements, any positive key predicted via the EUR is by definition 1sDI [119, 121]. The device independence does not necessarily extend to the heterodyne based protocols. This is because the steering demonstration requires a measurement choice by the untrusted party [129] which doesn't occur with heterodyne detection. Therefore employing heterodyne on the untrusted side invalidates the device independence. The extension to P&M schemes can also be made for direct reconciliation protocols where Alice controls the source through their equivalence to the EB schemes. This means that it is possible to generate a positive key using the coherent state protocol with homodyne detection which is a remarkable result. The device independence protocols are summarised in the inset table of Fig. 7.1.

The key rates found using the entropic proofs result in a different and generally lower secret key rates than the standard security proofs for the Gaussian protocols. To map out the ultimate limit of these protocols an idealised setup was modelled. As was done in Sec. 5.3 the channel was modelled as a Gaussian channel with a transmission T and excess noise parameter relative to the input of ξ. Each protocol was modelled as having a source with 17dB of entanglement and imperfections from measurement with finite effects were ignored. In Fig. 7.1 the secure region for each of the six protocols are identified to be 1sDI (there are two redundancies between P&M and EB schemes). The best performing protocol is the RR EPR scheme where both Alice and Bob use homodyne detectors. This scheme is secure up to a loss of 73%. The DR equivalent and the squeezed state with heterodyne protocol perform similarly for low noise channels. The worst performer is the coherent state protocol with Bob performing homodyne measurement. This protocol is only capable of a secure key up 33% loss in a low noise channel.

The standard security proofs for the Gaussian protocols, with an idealised very low noise channels, can tolerate arbitrarily large loss. This is in contrast to the results in

Fig. 7.1 which show that the 1sDI protocols discussed here are loss limited with low noise channels. This is due to the key rate found in Eq. (7.7) only being tight when the parties included can be approximated as sharing a pure, highly-squeezed EPR state [93, 119]. In a real QKD protocol this is rarely the case and the EUR method tends to give a pessimistic bound on the eavesdroppers information.

7.2.2 Link to EPR steering

The connection between 1sDI QKD protocols and asymmetric EPR steering has been made in the past for 1sDI DV QKD protocols [95] where it was shown to be a condition for a positive key rate. Like the 1sDI DV protocol the key rate for the CV 1sDI protocols found here can also be related to steering. The demonstration of EPR steering for CV is traditionally shown by the violation of the condition $\mathcal{E}_{\blacktriangleright} = V^X_{\mathrm{B|A}} V^P_{\mathrm{B|A}} \geq 1$ [130] to show Alice steered Bob. Their roles can be interchanged to show the opposite, $\mathcal{E}_{\blacktriangleleft}$. Consider Eq. (7.7) where $\beta = 1$. The key rate simplifies to,

$$K^{\triangleleft} \geq \log \frac{2}{e\sqrt{V^X_{\mathrm{B|A}} V^P_{\mathrm{B|A}}}} \tag{7.8}$$

$$= \log \frac{2}{e\sqrt{\mathcal{E}_{\blacktriangleright}}}. \tag{7.9}$$

The key rate will be positive if and only if $\mathcal{E}_{\blacktriangleright} < (\frac{2}{e})^2 \approx 0.54$. with the identical relation between the DR key rate and $\mathcal{E}_{\blacktriangleleft}$. In other words the condition for a positive 1sDI key rate is more stringent than EPR steering as is the case for 1sDI DV QKD [95]. For the protocols where a trusted heterodyne detection is used, the security of the protocol is instead linked to the steerability of the outcome of the heterodyne measurement, which will be more challenging due to the extra loss involved (see ref. [17]). Consequently this connection gives the operational interpretation for the Reid product of conditional variances [130] as being directly related to the number of secure 1sDI bits extractable from Gaussian states with Gaussian measurements. Interestingly, the gap between a steering violation and generation of a 1sDI key reveals that Eve's optimal attack allows her to steer the Gaussian measurement results of Alice and Bob.

7.3 Experiment

Of the six possible 1sDI protocols five were demonstrated with only three yielding a positive key. All four of the possible 1sDI entanglement based protocols were implemented along with a prepare and measure implementation of the coherent state protocol with

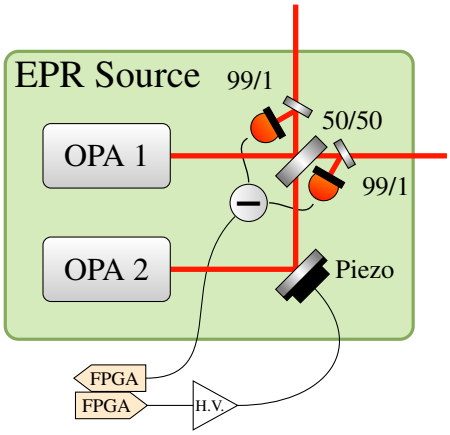


Figure 7.3: The EPR source used for the 1sDI CV QKD demonstration. Two OPA's are mixed on a 50/50 BS in quadrature. One mode is sent to Alice and the other is sent to Bob through a simulated loss channel as shown in Fig. 7.4. The squeezed beams are locked in quadrature by tapping off 1% of the power in each beam path after the BS and then using difference detection to control the piezo using the controller described in Sec. 2.4.2.

homodyne detection. The entanglement based squeezed state with homodyne protocols were the only EB protocols to give a positive key rate. They will be the focus of this chapter. The details of the prepare and measure protocol are given in Ref. [17, 131, 132].

For each EB protocol the same EPR source was used as described in Ch. 4 where two squeezed beams are interfered on a $50/50$ BS. For this experiment the EPR source was required to produce large correlations. To do this the regenerative gain of the two squeezers was increased so each one produced a squeezed state with roughly 6 dB of squeezing and 10.7 dB of anti-squeezing. The schematic of the entanglement source is shown in Fig. 7.3. One mode from the EPR source was directly measured by Alice and the other mode was sent through a Gaussian channel. For this experiment a simulated channel made using a PBS and halfwave plate to simplify the complexity. By changing the angle of the halfwave plate a loss of T was created on Bob's mode after the PBS.

Of the four EB protocols only two produced a positive key rate, the squeezed state protocols with homodyne detection, shown in Fig. 7.4 for both DR and RR. The noise in the EPR state introduced by the anti-squeezing was enough to reduce the correlations below the steering threshold required for a positive key when a heterodyne detector was used. Around 7 db of pure squeezing would be required for the two heterodyne protocols to achieve a positive key. The advantage of the P&M implementation of the DR coherent state protocol is in the ease of implementation. The modulation produced less noise and the variance of the output state can easily be finely tuned to suite the channel parameters. On the other hand EB protocols require a EPR resource which are difficult to build and don't offer the same fine controls on excess noise and state variance. It is worth pointing

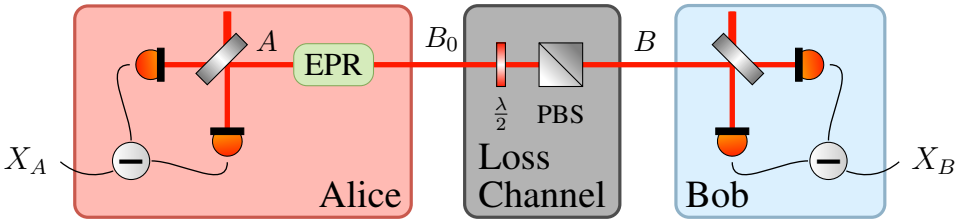


Figure 7.4: A simple schematic of the entanglement based 1sDI CV QKD experiment. An EPR state is distributed between Alice and Bob. Both states are measured using homodyne detection. Bob's state is passed through a simulated loss channel made from a halfwave plate and a PBS. The EPR source is shown in Fig. 7.3.

out that if the squeezer presented in Ch. 3 were used to produce an EPR state a positive key rate would be possible but the range would still be less than the P&M implementation even with fine tuning of the squeezing parameter.

7.3.1 Modelling

A model of squeezed state with homodyne measurement demonstration can be constructed using the phase space representation described in Sec. 1.4 as was done for the CV Bell test in Ch. 4. Here there is only a BS operation and three CP-Maps to model the loss channel and the loss on each homodyne. The model can be written as,

$$\gamma_{\text{out}} = \eta_{\text{A}}\eta_{\text{B}}T_{\text{Ch.}}S_{\text{BS}}\gamma_{\text{in}}S_{\text{BS}}^{T} + (1 - \eta_{\text{A}}\eta_{\text{B}}T)\mathbb{I}, \tag{7.10}$$

where η_{A} and η_{B} is the loss from the homodyne detection and T is the channel transmission. The input state covariance, γ_{in}, is given in Eq. (4.8).

7.4 Results

The key rates calculated from Eq. (7.7) with $\beta = 95\%$ for the protocols experimentally demonstrated to be secure are shown in Fig. 7.5. The loss in Fig. 7.5 is expressed as the equivalent transmission distance through standard single mode telecom optical fibre with a loss of 0.2 dB/km. Of the successfully demonstrated protocols as expected the RR squeezed state protocol with homodyne detection proved to be the most loss tolerant with a maximum demonstrated range of 7.57 ± 0.26 km. In contrast the DR squeezed state protocol performed the worst with a maximum range of only 2.52 ± 0.2 km. The DR coherent state protocol was able to achieve a demonstrated distance of 3.47 ± 0.46 km. A greater distance than would be possible even if the OPA presented in Ch. 3 were used.

Each parameter in the model, Eq. (7.10), was directly measured. The model was

then compared against the experimentally obtained data and was shown to be a good fit as shown in Fig. 7.5. The model demonstrated that the successful EB protocols could reach a maximum of 2.8 km for DR and 8 km for RR. The model was also used for understanding the limitations of the experiment. For the EB protocols the dominating limitation was from the intra-cavity losses in the OPA cavities. With a reasonable improvement to the cavity and detection losses it would be possible to extend the EB protocols to 8 and 17 km respectively [17].

The security proof presented in this chapter could be extended to include more finite-size effect and compared to the results in Ref. [119, 121, 126]. In particular, in the experiment in Ref. [126], the authors follow a similar program of applying entropic uncertainty relations, in this case to the smooth min entropies, allowing them to account for all finite-size effects while providing proof against complete general attacks. Their implementation was of the EB squeezed state with homodyne detection protocol. With better a better squeezing source their demonstration was able to demonstrate a distance of 2.7 km. Unlike the security proof presented here which spans RR and DR protocols their security proof is only valid for DR.

7.5 Conclusion

In summary this chapter detailed the derivation of a 1sDI security proof for the family of Gaussian protocols. Through experimental demonstrations three of these protocols were shown to produce a positive key achieving a maximum distance of 7.5 km of equivalent loss in an optical fibre. Although not extensively discussed in this chapter it was the first time a 1sDI coherent state QKD protocol has been demonstrated. An interesting result given the link between EPR steering and the 1sDI key rate. With the ease of which a P&M protocol can be implemented it would be an attractive option to investigate further.

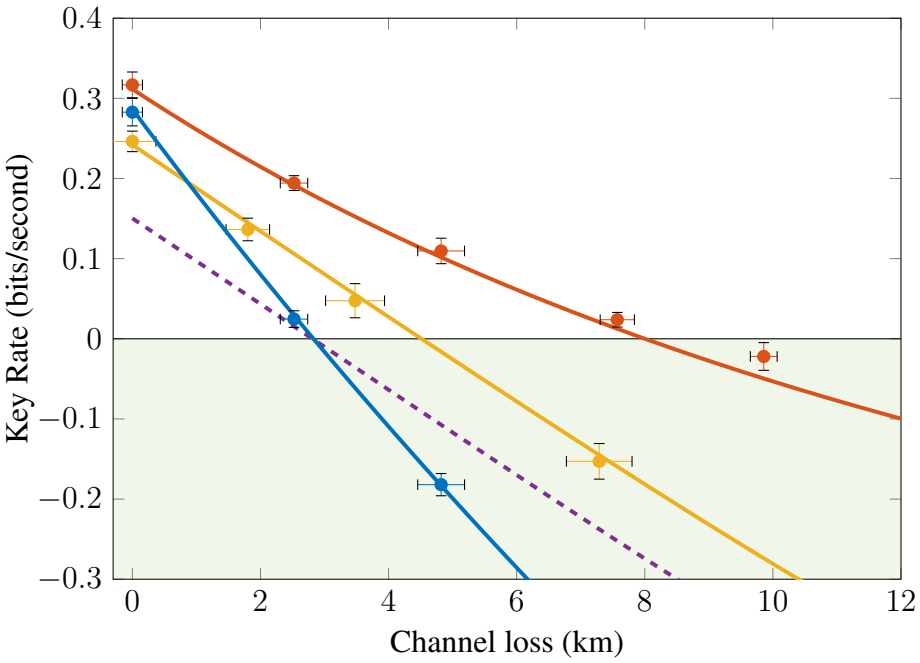


Figure 7.5: Experimentally obtained key rates (points) with a model fitted to the data (lines) vs effective distance through optical fiber for reverse (red) and direct (blue) reconciliation for the squeezed state protocols and direct reconciliation for the coherent state protocol (yellow). The effective distance was calculated based on a loss of 0.2dB/km through a single mode optical fiber. For RR a maximum distance of 7.57 ± 0.26 km was demonstrated with a predicted maximum range of 8 km. For DR the maximum demonstrated distance was 2.52 ± 0.2 km with a predicted maximum range of 2.8 km. The predicted performance of an optimised protocol using a model from the squeezer presented in Ch. 3 is also shown (purple dashed).

Chapter 8

Conclusion

8.1 Summary of Key results

In this thesis I have present results of the development of a low intra-cavity loss squeezer, the first optical CV Bell test using Gaussian measurements and a deterministic source, two new estimators for the channel noise in a CV QKD protocol and a family of 1sDI CV QKD prtocols. Each of these results build towards the contributions of this thesis to the next generation of QKD protocols. What follows is a summary of those results:

8.1.1 Quantum state generation

Squeezed state generation

Squeezed state forms the basic resource state for all of the experimental work presented in this thesis and in many other experiments. Here the key result is the observation of 11 dB of vacuum squeezing with around 580 mW of pump power. This figure is corrected for the dark noise on the detector. To improve the squeezing both a better locking method will be investigated and the non-linear crystal will be recoated. In the near future this squeezer will be used for a probabilistic squeeze gate.

CV Bell test

The Bell inequality, originally formulated for DV, is violated for the first time using optical CV states. While this demonstration falls short of the four discrete variable loop-hole free Bell test this is still a significant milestone in the development of technologies based on CV optics. The maximum violation of the Bell inequality observed was $|B| = 2.31$ 15 standard deviations above 2 and a correlation fringe visibility of 75%. The methodology used in this experiment can could be used for a source independent QRNG or QKD as the detection process needs to be trusted for this particular implementation.

8.1.2 CV QKD

Channel parameter estimation

This chapter discussed the results a investigation use of the method of moments estimator with CV QKD to estimate the channel noise relative to the output. Two new estimators were proposed that outperformed in terms of variance for high loss channels the maximum likelihood estimator that has been previously used. The performance of these two estimators was evaluated with the coherent state protocol with homodyne detection. The method of moments estimator is simple enough that it would be easy to modify for other protocols or include more parameters

One side device independent CV QKD

Using a tripartite EUP six 1sDI CV QKD protocols was found from the family of Gaussin CV QKD protocols. The security proof for the squeezed state protocol was derived with an experimental demonstration. The original work also included a demonstration of the P&M coherent state protocol with homodyne detection. This was the first time a protocol of that type had been demonstrated. The EB equivilent was also attempted but failed to produce a positive key rate due to excess noise and not enough squeezing from the source. Both problems that would be solved with the OPA in Ch. 3. The demonstration achieved a maximum equivalent distance through an optical fiber of 7.57 ± 0.25 km for RR and 2.52 ± 0.2 km for DR. The P&M protocol achieved 3.47 ± 0.46, which is still further than the predicted performance with the OPA from Ch. 3.

8.2 Outlook

It is an exciting time to be involved in quantum optics. With the four loop-hole free Bell tests that have recently been demonstrated there is more evidence suggesting quantum mechanics is an accurate description of reality. The loop-hole free Bell tests also open up the opportunity for real DI QKD and DI QRNG protocols. So far these results have been limited to DV protocols but with the demonstration of a CV Bell test here and with a number of proposed CV Bell test protocols claiming to be loop-hole free DI might in the future extend to CV. Here the protocols will be able to take advantage of the high bandwidth, room temperature low loss detection and deterministic sources.

Recently there was also a demonstration of entanglement between two sites 1203 km apart with the source in orbit around earth at an altitude ranging from 1600 to 2400 km [133]. This is part of an effort to extend QKD into a protocol that has a global reach.

There are a number of groups trying to achieve this same goal using both CV and DV. If it works then QKD will be much more useful in the field.

One avenue of investigation for the range of QKD to be extend is to place realistic limits on Eve using a noisy storage model. For many previously demonstrated CV protocols Eve is assumed to be all powerful and capable of making the optimal attack [106, 108]. This probably is not the case in a real situation where the attackers are likely to be human. Application of noisy storage models to QKD protocols has been demonstrated for DV [134–136].

Appendix

Appendix A

Electronics

A.1 Photodetector

The basic circuit of a transimpedance amplifier is given in Fig. A.1. The advantage of the transimpedance amplifier over a simple resistor circuit is that it is a low impedance to the diode which allows for higher gains. A simple resistor would present as a large impedance with high gains. The op-amp will try to match the potential at its inverting and non-inverting input, which is grounded, by using the feedback resistor. This cause the output of the transimpedance stage to be $V_{\text{out}} = i_d R_f$ at DC. The diode will naturally contribute some parasitic capacitance. With the feedback resistor this creates a low pass filter in the feedback which causes an oscillation peak on the output. The compensation capacitor C_f reduces this peak by providing a zero in the transfer function to cancel it out. More detailed calculations are given in Ref. [36].

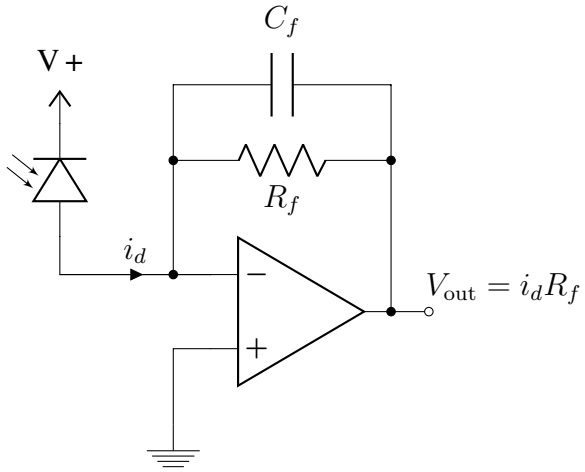


Figure A.1: Basic circuit for a transimpedance amplifier. The negative input will present as a low impedance to i_d. The op-amp will try to match the potential of both inputs through R_f by driving the output voltage giving a DC transimpedance gain of R_f.

A.2 Piezo driver

Part of the work found in Ch. 3 led to the opportunity to use more modern Piezo actuators that had previously been used in the group. Since the last major purchase of Piezo devices the voltages required to drive them to their maximum displacement have dropped from +400V to +150V. The displacement of the new Piezos was also found to be such that the DAC with a range of $\pm 10V$ on the FPGA was sufficient to be able to scan the cavities nearly a full FSR with a low frequency. For these new Piezo devices a cheaper low noise HV amp was developed. The previous HV amps used to drive the Piezos were based around the PA85 which while good are expensive and beyond the needs for this application. The PDu150 from PiezoDrive [137] was found to be an acceptable alternative through a little easy to break because of its power supply design.

A design was made using same LTC6090 op-amp as the PDu150 with a gain of 6. The design was refined with help from the Electronics Unit at RSPE to include high voltage input protection. The final design is given in Fig. A.2. The op-amp has a full power bandwidth of 65Hz with a capacitive load of 2.64uF and a supply voltage of -15V to +100V. The small signal bandwidth is 47 kHz is sufficient for control of the cavities in Ch. 3. To increase the bandwidth either the design could be changed to use dual op-amps to push and pull the voltage or the output resister could be reduced. Reducing the output resister would also reduce the full power bandwidth. For high bandwidth control the PA85 based amplifier would be preferable.

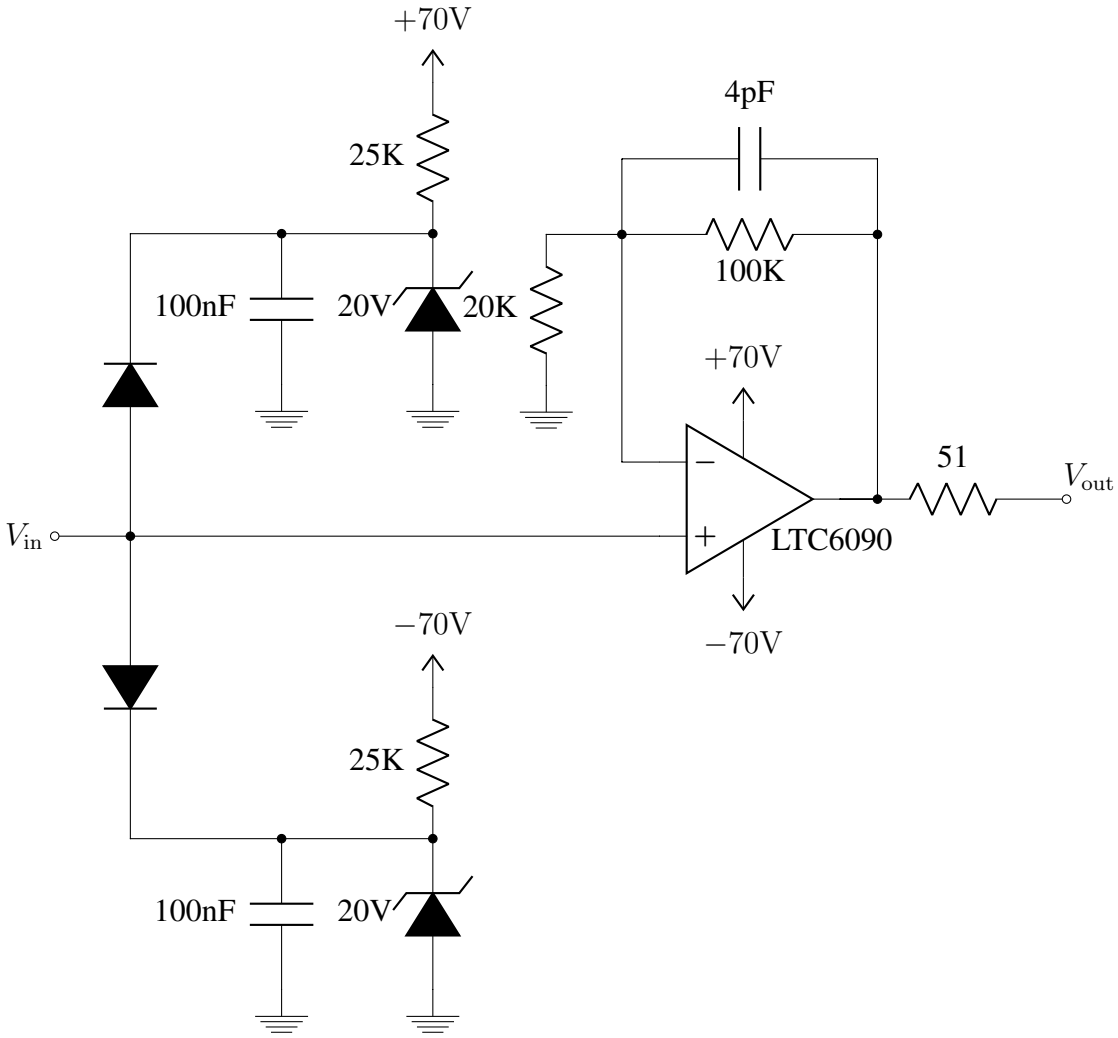


Figure A.2: LTC6090 high voltage amplifier circuit with input protection diodes with a gain of 6.

Appendix B

Modifications to the FPGA locking code

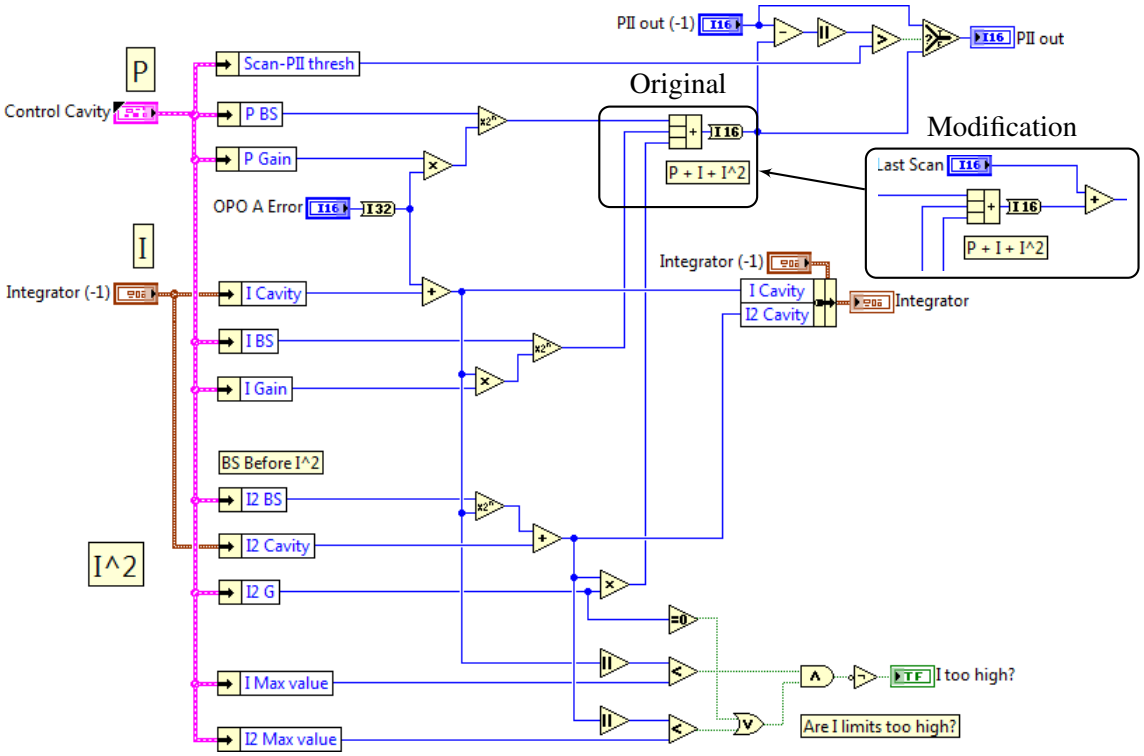


Figure B.1: A modification to PII controller from Ref. [46]. The intended operation of the code is to scan the plant to near the locking point and then engage the PII controller. The original design of the controller had no way of knowing where the locking point was in the scan. This resulted in the PII controller trying to lock with the initial point of the scan. The modification offsets the output from the PII controller by the last scan value (call out box) which will be close to the locking point.

Appendix C

Raw spectrum of the OPA homodyne measurements

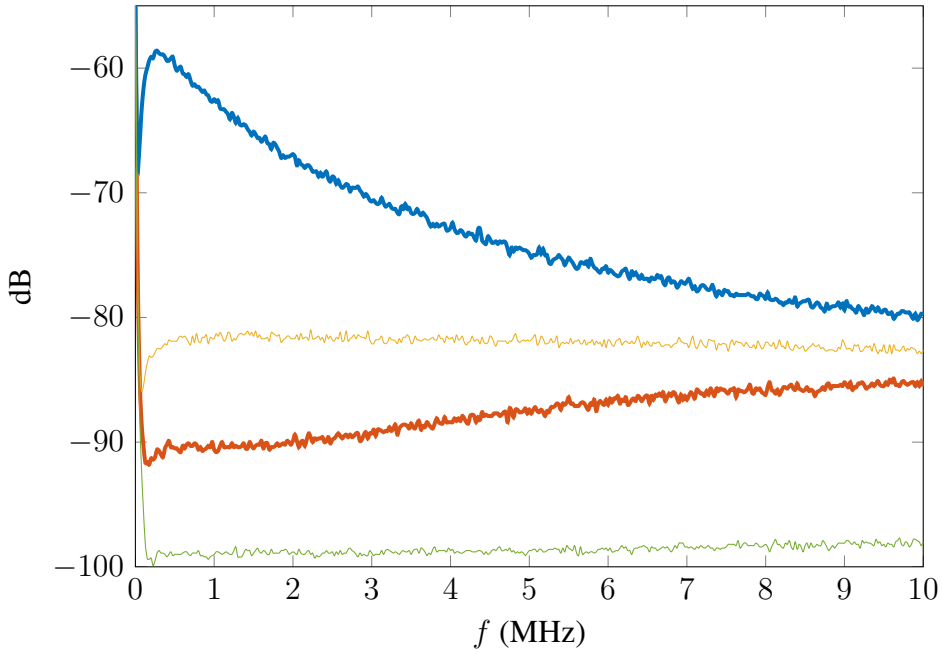


Figure C.1: Raw squeezing data from the spectrum analyser for the OPA in Ch. 3 with the miss-aligned pump. The dark noise(green), squeezed quadrature (red), shot noise (yellow) and anti-squeezed quadrature (blue) are shown.

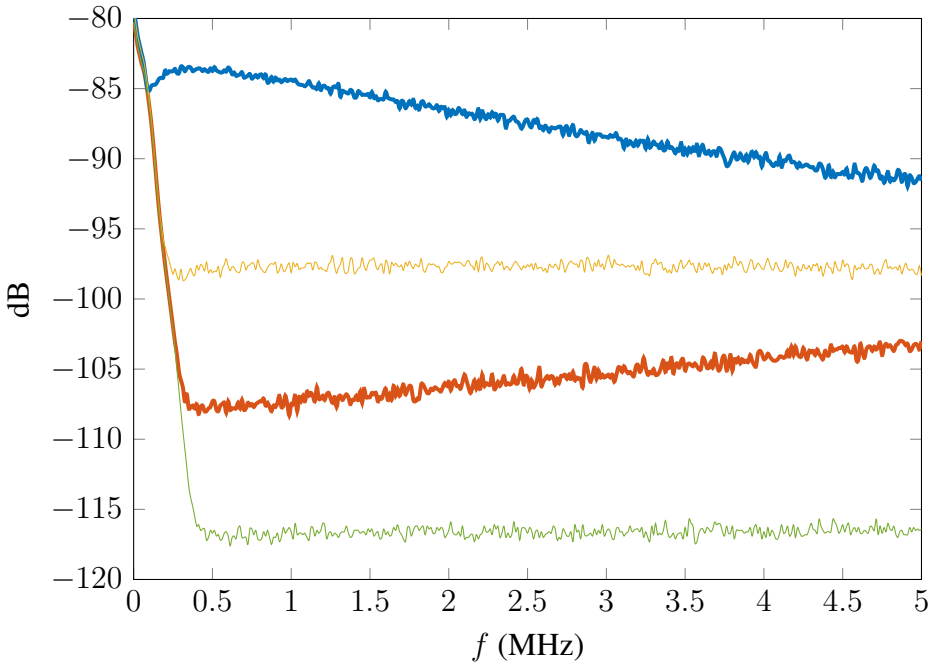


Figure C.2: Raw squeezing data from the spectrum analyser for the OPA in Ch. 3 with the correctly aligned pump. The dark noise(green), squeezed quadrature (red), shot noise (yellow) and anti-squeezed quadrature (blue) are shown. The anti-squeezing measurement was not locked on the correct quadrature.

Appendix D

Additional channel noise parameter estimator calculations

D.1 Variance of $\hat{\sigma}^2_{\mathrm{mm}}$

Using the same method described in Sec. 6.4 the variance for $\hat{\sigma}^2_{\mathrm{mm}}$ is given by

$$\mathrm{Var}(\hat{\sigma}^2_{\mathrm{mm}}) \approx \frac{2\sigma^4}{N} + \frac{2t^4V_A^2}{N} + \left(\frac{1}{m} - \frac{1}{N}\right) 4t^2\sigma^2 V_A. \tag{D.1}$$

Here the covariance C_J can be found using App. D.2.1 and setting the appropriate values to 0. With Eq. (D.1) we find

$$\mathrm{Var}(\hat{\sigma}^2_{\mathrm{mm}}) = \frac{2t^4V_A^2}{N} + \mathrm{Var}(\hat{\sigma}^2_{\mathrm{MM}}). \tag{D.2}$$

This agrees with the claim that $\mathrm{Var}(\hat{\sigma}^2_{\mathrm{mm}}) > \mathrm{Var}(\hat{\sigma}^2_{\mathrm{MM}})$.

D.2 Elements of C_J

D.2.1 C_J for $\hat{\sigma}^2_{\mathrm{MM}}$

The diagonal terms for the covariance matrix C_J for the estimator $\hat{\sigma}_{\mathrm{MM}}$ are given by,

$$\mathrm{Var}(\hat{\sigma}^2_{\mathrm{A}}) = \frac{2\sigma^4_{\mathrm{A}}}{N}, \qquad \mathrm{Var}(\hat{\sigma}^2_{\mathrm{A}'}) = \frac{2\sigma^4_{\mathrm{A}'}}{m},$$
$$\mathrm{Var}(\hat{\sigma}^2_{\mathrm{B}}) = \frac{2\sigma^4_{\mathrm{B}}}{N} \qquad \text{and} \quad \mathrm{Var}(\hat{\sigma}_{\mathrm{A}'\mathrm{B}'}) = \frac{1}{m}(2t^2\sigma^4_{\mathrm{A}'} + \sigma^2\sigma^2_{\mathrm{A}'}).$$

The off diagonal terms are given by,

$$\begin{aligned}
\mathrm{Cov}(\hat{\sigma}^2_{\mathrm{A}}, \hat{\sigma}^2_{\mathrm{B}}) &= 2t^2\frac{\sigma^4_{\mathrm{A}}}{N}, & \mathrm{Cov}(\hat{\sigma}^2_{\mathrm{A}}, \hat{\sigma}^2_{\mathrm{A}'}) &= 2\frac{\sigma^4_{\mathrm{A}'}}{N},\\
\mathrm{Cov}(\hat{\sigma}^2_{\mathrm{A}}, \hat{\sigma}_{\mathrm{A}'\mathrm{B}'}) &= 2t\frac{\sigma^4_{\mathrm{A}'}}{N}, & \mathrm{Cov}(\hat{\sigma}^2_{\mathrm{A}'}, \hat{\sigma}_{\mathrm{A}'\mathrm{B}'}) &= 2t\frac{\sigma^4_{\mathrm{A}'}}{m},\\
\mathrm{Cov}(\hat{\sigma}^2_{\mathrm{B}}, \hat{\sigma}^2_{\mathrm{A}'}) &= 2t^2\frac{\sigma^4_{\mathrm{A}'}}{N}
\end{aligned}$$

and

$$\mathrm{Cov}(\hat{\sigma}^2_{\mathrm{B}}, \hat{\sigma}_{\mathrm{A}'\mathrm{B}'}) = 2t\frac{t^2\sigma^4_{\mathrm{A}'} + \sigma^2\sigma^2_{\mathrm{A}'}}{N}.$$

D.2.2 C_J for $\hat{\sigma}^2_{\mathrm{MM}''}$

The diagonal terms for the covariance matrix C_J for the estimator $\hat{\sigma}_{\mathrm{MM}''}$ are given by,

$$\begin{aligned}
\mathrm{Var}(\hat{\sigma}^2_{\mathrm{A}''}) &= \frac{2\sigma^4_{\mathrm{A}''}}{n}, & \mathrm{Var}(\hat{\sigma}^2_{\mathrm{A}'}) &= \frac{2\sigma^4_{\mathrm{A}'}}{m},\\
\mathrm{Var}(\hat{\sigma}^2_{\mathrm{B}''}) &= \frac{2\sigma^4_{\mathrm{B}''}}{n} & \text{and} \quad \mathrm{Var}(\hat{\sigma}_{\mathrm{A}'\mathrm{B}'}) &= \frac{1}{m}(2t^2\sigma^4_{\mathrm{A}'} + \sigma^2\sigma^2_{\mathrm{A}'})
\end{aligned}$$

The off diagonal terms are given by,

$$\begin{aligned}
\mathrm{Cov}(\hat{\sigma}^2_{\mathrm{A}''}, \hat{\sigma}^2_{\mathrm{B}''}) &= 2t^2\frac{\hat{\sigma}^4_{\mathrm{A}''}}{N}, & \mathrm{Cov}(\hat{\sigma}^2_{\mathrm{A}''}, \hat{\sigma}^2_{\mathrm{A}'}) &= 0,\\
\mathrm{Cov}(\hat{\sigma}^2_{\mathrm{A}''}, \hat{\sigma}_{\mathrm{A}'\mathrm{B}'}) &= 0, & \mathrm{Cov}(\hat{\sigma}^2_{\mathrm{A}'}, \hat{\sigma}_{\mathrm{A}'\mathrm{B}'}) &= 2t\frac{\sigma^4_{\mathrm{A}'}}{m},\\
\mathrm{Cov}(\hat{\sigma}^2_{\mathrm{B}''}, \hat{\sigma}^2_{\mathrm{A}'}) &= 0 \quad \text{and} & \mathrm{Cov}(\hat{\sigma}^2_{\mathrm{B}''}, \hat{\sigma}^2_{\mathrm{A}'\mathrm{B}'}) &= 0.
\end{aligned}$$

Here A'' and B'' to indicate the statistic was calculated using the n subset of states used for generating the final key.

D.3 The optimal estimator

An optimal estimator can be found from a linear combination of two estimators, $\hat{\theta}_1$ and $\hat{\theta}$, with $\mathrm{Cov}(\hat{\theta}_1, \hat{\theta}_2) = 0$. The optimal estimator is given by,

$$\hat{\theta}_{\mathrm{opt}} = \alpha\hat{\theta}_1 + (1-\alpha)\hat{\theta}_2 \tag{D.3}$$

with a variance of,

$$\mathrm{Var}(\hat{\theta}_{\mathrm{opt}}) = \alpha^2 \mathrm{Var}(\hat{\theta}_1) + (1-\alpha)^2 \mathrm{Var}(\hat{\theta}_2) \tag{D.4}$$

which is a convex function of α. The optimal value of α can be found by minimising $\mathrm{Var}(\hat{\theta}_{\mathrm{opt}})$.

$$0 = \frac{d}{d\alpha}\mathrm{Var}(\hat{\theta}_{\mathrm{opt}}) \tag{D.5}$$

$$0 = 2\alpha\mathrm{Var}(\hat{\theta}_1) - 2\mathrm{Var}(\hat{\theta}_2) + 2\alpha\mathrm{Var}(\hat{\theta}_2) \tag{D.6}$$

$$\alpha = \frac{\mathrm{Var}(\hat{\theta}_2)}{\mathrm{Var}(\hat{\theta}_1) + \mathrm{Var}(\hat{\theta}_2)}. \tag{D.7}$$

D.3.1 Covariance of $\hat{\sigma}^2_{\mathrm{MLE}}$ and $\hat{\sigma}^2_{\mathrm{MM}''}$

We can show that $\mathrm{Cov}(\hat{\sigma}^2_{\mathrm{MM}''}, \hat{\sigma}_{\mathrm{MLE}}) = 0$ given that $\mathrm{Cov}(\hat{\sigma}^2_{\mathrm{B}''}, \hat{\sigma}^2_{\mathrm{MLE}}) = 0$, $\mathrm{Cov}(\hat{\sigma}^2_{\mathrm{A}''}, \hat{\sigma}^2_{\mathrm{MLE}}) = 0$ and $\mathrm{Cov}(\hat{t}, \hat{\sigma}^2_{\mathrm{MLE}}) = 0$ [116]

$$\mathrm{Cov}(\hat{\sigma}^2_{\mathrm{MM}''}, \hat{\sigma}_{\mathrm{MLE}}) = \mathrm{Cov}(\hat{\sigma}^2_{\mathrm{B}''} - \hat{t}^2\hat{\sigma}^2_{\mathrm{A}''}, \hat{\sigma}^2_{\mathrm{MLE}}) \tag{D.8}$$

$$= \mathrm{Cov}(\hat{\sigma}^2_{\mathrm{B}''}, \hat{\sigma}^2_{\mathrm{MLE}}) - \mathrm{Cov}(t^2\hat{\sigma}^2_{\mathrm{A}''}, \hat{\sigma}^2_{\mathrm{MLE}}) \tag{D.9}$$

$$= 0. \tag{D.10}$$

Bibliography

[1] A. Einstein, B. Podolsky, and N. Rosen, Physical Review **47**, 777 (1935).

[2] J. S. Bell, Physics **1**, 195 (1964).

[3] A. Aspect, P. Grangier, and G. Roger, Physical Review Letters **49**, 91 (1982).

[4] M. Giustina et al., Physical Review Letters **115**, 250401 (2015).

[5] B. Hensen et al., Nature **526**, 682 (2015).

[6] L. K. Shalm et al., Physical Review Letters **115**, 250402 (2015).

[7] W. Rosenfeld, D. Burchardt, R. Garthoff, K. Redeker, N. Ortegel, M. Rau, and H. Weinfurter, Physical Review Letters **119**, 010402 (2017).

[8] S. L. Braunstein and P. van Loock, Reviews of Modern Physics **77**, 513 (2005).

[9] C. H. Bennett and S. J. Wiesner, Physical Review Letters **69**, 2881 (1992).

[10] T. C. Ralph, Physical Review A **61**, 010303 (1999).

[11] T. Symul, S. M. Assad, and P. K. Lam, Applied Physics Letters **98**, 231103 (2011).

[12] W. Diffie and M. Hellman, IEEE transactions on Information Theory **22**, 644 (1976).

[13] M. A. Nielsen and I. L. Chuang, *Quantum computation and quantum information*, 10th anniversary ed. (Cambridge University Press, 2010).

[14] C. H. Bennett and G. Brassard, eds., *Proceedings of IEEE. International Conference on Computers Systems & Signal Processing* (IEEE, 1984), 175-179.

[15] F. Grosshans and P. Grangier, Physical Review Letters **88**, 057902 (2002).

[16] NIST, *NIST Computer Security Resource Center*, (2016) `http://csrc.nist.gov/groups/ST/post-quantum-crypto/` (visited on 06/06/2017).

[17] N. Walk et al., Optica **3**, 634 (2016).

[18] S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Massar, and V. Scarani, New Journal of Physics **11**, 045021 (2009).

[19] D. F. Walls and G. J. Milburn, *Quantum optics*, Second edition., Previous edition: 1995. (Springer, 2008).

[20] H.-A. Bachor and T. C. Ralph, *A guide to experiments in quantum optics*, Second, revised and enlarged edition., Physics textbook, Includes bibliographical references and index. (Wiley-VCH, 2004).

[21] W. P. Bowen, "Experiments towards a Quantum Information Network with Squeezed Light and Entanglement" (2003).

[22] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, Reviews of Modern Physics **86**, 419 (2014).

[23] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Physical Review Letters **23**, 880 (1969).

[24] B. S. Cirel'son, Letters in Mathematical Physics **4**, 93 (1980).

[25] A. Aspect, J. Dalibard, and G. Roger, Physical Review Letters **49**, 1804 (1982).

[26] P. M. Pearle, Physical Review D **2**, 1418 (1970).

[27] A. Furusawa, *Quantum States of Light*, 1st ed., Vol. 10, SpringerBriefs in Mathematical Physics (Springer Japan, 2015).

[28] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, Reviews of Modern Physics **84**, 621 (2012).

[29] R. G.-P. Sanchez, "Quantum Information with Optical Continuous Variables: from Bell Tests to Key Distribution" (Universite Libre de Bruxelles, 2007).

[30] U. Leonhardt, *Measuring the quantum state of light*, Cambridge studies in modern optics (Cambridge University Press, 1997), 194 pp.

[31] M. G. A. Paris, F. Illuminati, A. Serafini, and S. De Siena, Physical Review A **68**, 012314 (2003).

[32] C. M. Caves and B. L. Schumaker, Physical Review A **31**, 3068 (1985).

[33] B. L. Schumaker and C. M. Caves, Physical Review A **31**, 3093 (1985).

[34] N. Grosse, "Harmonic Entanglement and Photon Anti-Bunching" (2009).

[35] B. C. Buchler, "Electro-optic control of quantum measurements" (ANU, 2001).

[36] P. Horowitz and H. Winfield, *The art of electronics*, Third edition (Cambridge University Press, 2015), 1192 pp.

[37] J. Eisert, S. Scheel, and M. B. Plenio, Physical Review Letters **89**, 137903 (2002).

[38] K. Wagner, J. Janousek, V. Delaubert, H. Zou, C. Harb, N. Treps, J. F. Morizur, P. K. Lam, and H. A. Bachor, Science **321**, 541 (2008).

[39] M. Lassen, V. Delaubert, J. Janousek, K. Wagner, H.-A. Bachor, P. K. Lam, N. Treps, P. Buchhave, C. Fabre, and C. C. Harb, Physical Review Letters **98**, 083602 (2007).

[40] J. Janousek, "Investigation of non-classical light and its application in ultrasensitive measurements" (2007).

[41] C. W. Gardiner and M. J. Collett, Physical Review A **31**, 3761 (1985).

[42] J. A. Armstrong, N. Bloembergen, J. Ducuing, and P. S. Pershan, Physical Review **127**, 1918 (1962).

[43] M. J. Collett and C. W. Gardiner, Physical Review A **30**, 1386 (1984).

[44] E. D. Black, American Journal of Physics **69**, 79 (2001).

[45] B. Hage, "Purification and Distillation of Continuous Variable Entanglement" (2010).

[46] S. Armstrong, *PI-state-4-phase-locks: A state-machine architecture to control 4 optical phase locks via PI controllers*, Sept. 17, 2014.

[47] S. Armstrong, "Experiments in quantum optics: Scalable entangled states and quantum computation with cluster states", PhD thesis (2014).

[48] K. Yang, G. Zhu, Q. Hao, K. Huang, J. Laurat, W. Li, and H. Zeng, IEEE Photonics Technology Letters **28**, 2129 (2016).

[49] K. Huang, H. Le Jeannic, J. Ruaudel, O. Morin, and J. Laurat, Review of Scientific Instruments **85**, 123112 (2014).

[50] S. L. Braunstein and H. J. Kimble, Physical Review A **61**, 042302 (2000).

[51] J. Jing, J. Zhang, Y. Yan, F. Zhao, C. Xie, and K. Peng, Physical Review Letters **90**, 167903 (2003).

[52] H. Yonezawa et al., Science **337**, 1514 (2012).

[53] J. Aasi et al., Nature Photonics **7**, 613 (2013).

[54] T. L. S. Collaboration, Nature Physics **7**, 962 (2011).

[55] U. L. Andersen, T. Gehring, C. Marquardt, and G. Leuchs, Physica Scripta **91**, 053001 (2016).

[56] H. Vahlbruch, M. Mehmet, K. Danzmann, and R. Schnabel, Physical Review Letters **117**, 110801 (2016).

[57] Y. Takeno, M. Yukawa, H. Yonezawa, and A. Furusawa, Optics Express **15**, 4321 (2007).

[58] M. Stefszky, "Generation and Detection of Low-Frequency Squeezing for Gravitational-Wave Detection" (2012).

[59] NKT Photonics A/S, *Koheras BASIK low noise single-frequency OEM lasers*, (2017) http://www.nktphotonics.com/product/koheras-basik-low-noise-single-frequency-oem-laser-modules/ (visited on 04/26/2017).

[60] NKT Photonics A/S, *Koheras Basik Module fiber laser, product type K83-242-73 Test Report* (Dec. 8, 2015).

[61] W. P. Bowen, R. Schnabel, N. Treps, H.-A. Bachor, and P. K. Lam, Journal of Optics B: Quantum and Semiclassical Optics **4**, 421 (2002).

[62] J. Steinlechner, S. Ast, C. Krüger, A. P. Singh, T. Eberle, V. Händchen, and R. Schnabel, Sensors **13**, 565 (2013).

[63] G. D. Boyd and D. A. Kleinman, Journal of Applied Physics **39**, 3597 (1968).

[64] H. Jeng, "Towards Quantum Teleportation Assisted by Noiseless Linear Optical Amlification", Honoursthesis (ANU, 2016).

[65] S. Sonar, *Second Harmonic Generation Summer Research Project* (ANU, 2016).

[66] K. McKenzie, E. E. Mikhailov, K. Goda, P. K. Lam, N. Grosse, M. B. Gray, Nergis Mavalvala, and D. E. McClelland, Journal of Optics B: Quantum and Semiclassical Optics **7**, S421 (2005).

[67] H. Vahlbruch, S. Chelkowski, B. Hage, A. Franzen, K. Danzmann, and R. Schnabel, Physical Review Letters **97**, 011101 (2006).

[68] E. Oelker, "Squeezed States for Adanced Gravitational Wave Detectors" (2016).

[69] N. C. Menicucci, Physical Review Letters **112**, 120504 (2014).

[70] J.-i. Yoshikawa, T. Hayashi, T. Akiyama, N. Takei, A. Huck, U. L. Andersen, and A. Furusawa, Physical Review A **76**, 060301 (2007).

[71] R. Filip, P. Marek, and U. L. Andersen, Physical Review A **71**, 042308 (2005).

[72] H. M. Chrzanowski, "Extracting quantum correlations from gaussian states", PhD thesis (ANU, 2014).

[73] S. M. Assad, *Improving the fidelity of a measurement base squeezing gate using a heralding protocol*, E-Mail, 2017.

[74] J. S. Bell and A. Aspect, *Speakable and unspeakable in quantum mechanics*, 2nd ed., Collected papers on quantum philosophy (Cambridge University Press, 2004).

[75] R. García-Patrón, J. Fiurášek, N. J. Cerf, J. Wenger, R. Tualle-Brouri, and P. Grangier, Physical Review Letters **93**, 130409 (2004).

[76] D. Cavalcanti, N. Brunner, P. Skrzypczyk, A. Salles, and V. Scarani, Physical Review A **84**, 022105 (2011).

[77] T. C. Ralph, W. J. Munro, and R. E. S. Polkinghorne, Physical Review Letters **85**, 2035 (2000).

[78] E. H. Huntington and T. C. Ralph, Physical Review A **65**, 012306 (2001).

[79] Z. Y. Ou and L. Mandel, Physical Review Letters **61**, 50 (1988).

[80] D. G. Marangon, G. Vallone, and P. Villoresi, Physical Review Letters **118**, 060503 (2017).

[81] Z. Cao, H. Zhou, X. Yuan, and X. Ma, Physical Review X **6**, 011020 (2016).

[82] V. Bužek and M. Hillery, Physical Review A **54**, 1844 (1996).

[83] J. Y. Haw, J. Zhao, J. Dias, S. M. Assad, M. Bradshaw, R. Blandino, T. Symul, T. C. Ralph, and P. K. Lam, Nature Communications **7**, ncomms13222 (2016).

[84] S. Singh, *The code book : the secret history of codes and codebreaking* (Fourth Estate, 2000).

[85] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Reviews of Modern Physics **81**, 1301 (2009).

[86] M. Herrero-Collantes and J. C. Garcia-Escartin, Reviews of Modern Physics **89**, 015004 (2017).

[87] Frederik De Wilde, *Frederik De Wilde Quantum Foam*, (2017) `http://frederik-de-wilde.com/project/quantum-foam/` (visited on 06/01/2017).

[88] O. Thearle, S. M. Assad, and T. Symul, Physical Review A **93**, 042343 (2016).

[89] C. E. Shannon, The Bell System Technical Journal **27**, 379 (1948).

[90] P. J. Coles, M. Berta, M. Tomamichel, and S. Wehner, Reviews of Modern Physics **89**, 015002 (2017).

[91] H. Maassen and J. B. M. Uffink, Physical Review Letters **60**, 1103 (1988).

[92] A. Ferenczi, "Security proof methods for quantum key distribution protocols" (UWSpace, 2013).

[93] F. Furrer, M. Berta, M. Tomamichel, V. B. Scholz, and M. Christandl, Journal of Mathematical Physics **55**, 122205 (2014).

[94] R. L. Frank and E. H. Lieb, Communications in Mathematical Physics **323**, 487 (2013).

[95] C. Branciard, E. G. Cavalcanti, S. P. Walborn, V. Scarani, and H. M. Wiseman, Physical Review A **85**, 010301 (2012).

[96] G. Vallone, D. G. Marangon, M. Tomasin, and P. Villoresi, Physical Review A **90**, 052327 (2014).

[97] P. Shor, SIAM Journal on Computing **26**, 1484 (1997).

[98] R. Dridi and H. Alghassi, Scientific Reports **7**, srep43048 (2017).

[99] G. Adj, I. Canales-Martínez, N. Cruz-Cortés, A. Menezes, T. Oliveira, L. Rivera-Zamarripa, and F. Rodríguez-Henríquez, *Computing discrete logarithms in cryptographically-interesting characteristic-three finite fields*, 914 (2016).

[100] W. K. Wootters and W. H. Zurek, Nature **299**, 802 (1982).

[101] F. Grosshans and P. Grangier, (2002).

[102] A. Leverrier and P. Grangier, Physical Review Letters **102**, 180504 (2009).

[103] A. Leverrier and P. Grangier, Physical Review A **81**, 062314 (2010).

[104] R. Renner and J. I. Cirac, Physical Review Letters **102**, 110504 (2009).

[105] J. Lodewyck et al., Physical Review A **76**, 042305 (2007).

[106] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, Nature Photonics **7**, 378 (2013).

[107] P. Jouguet, S. Kunz-Jacques, E. Diamanti, and A. Leverrier, Physical Review A **86**, 032309 (2012).

[108] D. Huang, P. Huang, D. Lin, and G. Zeng, Scientific Reports **6**, 19201 (2016).

[109] A. Leverrier, F. Grosshans, and P. Grangier, Physical Review A **81**, 062343 (2010).

[110] S. J. Johnson, A. M. Lance, L. Ong, M. Shirvanimoghaddam, T. C. Ralph, and T. Symul, New Journal of Physics **19**, 023003 (2017).

[111] P. Jouguet, S. Kunz-Jacques, and A. Leverrier, Physical Review A **84**, 062317 (2011).

[112] J. Müller-Quade and R. Renner, New Journal of Physics **11**, 085006 (2009).

[113] A. Leverrier, Physical Review Letters **114**, 070501 (2015).

[114] L. Ruppert, V. C. Usenko, and R. Filip, Physical Review A **90**, 062310 (2014).

[115] S. M. Kay, *Estimation Theory*, Vol. 1, Fundamentals of Statiscal Signal Processing (Prentice Hall, 1993).

[116] J. K. Patel and C. B. Read, *Handbook of the Normal Distribution*, 2nd ed., Statistics: Textbooks and Monographs (Marcel Dekker, Inc, 1996).

[117] J. Neter, W. Wasserman, and M. H. Kutner, *Applied Linear statistical model*, 3rd ed. (CRC Press, 1990).

[118] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, Nature Communications **3**, ncomms1631 (2012).

[119] F. Furrer, Physical Review A **90**, 042325 (2014).

[120] V. Scarani and R. Renner, Physical Review Letters **100**, 200501 (2008).

[121] F. Furrer, T. Franz, M. Berta, A. Leverrier, V. B. Scholz, M. Tomamichel, and R. F. Werner, Physical Review Letters **109**, 100502 (2012).

[122] J.-Z. Huang, C. Weedbrook, Z.-Q. Yin, S. Wang, H.-W. Li, W. Chen, G.-C. Guo, and Z.-F. Han, Physical Review A **87**, 062329 (2013).

[123] J.-Z. Huang, S. Kunz-Jacques, P. Jouguet, C. Weedbrook, Z.-Q. Yin, S. Wang, W. Chen, G.-C. Guo, and Z.-F. Han, Physical Review A **89**, 032304 (2014).

[124] X.-C. Ma, S.-H. Sun, M.-S. Jiang, and L.-M. Liang, Physical Review A **87**, 052309 (2013).

[125] H. Qin, R. Kumar, and R. Alléaume, Physical Review A **94**, 012325 (2016).

[126] T. Gehring, V. Händchen, J. Duhme, F. Furrer, T. Franz, C. Pacher, R. F. Werner, and R. Schnabel, Nature Communications **6**, ncomms9795 (2015).

[127] J. Barrett, Physical Review A **86** (2012) 10.1103/PhysRevA.86.062326.

[128] U. Vazirani, Physical Review Letters **113** (2014) 10.1103/PhysRevLett.113.140501.

[129] H. M. Wiseman, S. J. Jones, and A. C. Doherty, Physical Review Letters **98**, 140402 (2007).

[130] M. D. Reid, Physical Review A **40**, 913 (1989).

[131] S. Hosseini, "Quantum Discord, EPR Steering and Bell-type Correlations for Secure CV Quantum Communications" (2017).

[132] J. Haw, "Continuous Variable Optimisation of Quantum Randomness and Probabilistic Linear Amplificiation" (2017).

[133] J. Yin et al., Science **356**, 1140 (2017).

[134] S. Wehner, C. Schaffner, and B. M. Terhal, Physical Review Letters **100**, 220502 (2008).

[135] S. Wehner, M. Curty, C. Schaffner, and H.-K. Lo, Physical Review A **81**, 052336 (2010).

[136] C. Schaffner, Physical Review A **82**, 032308 (2010).

[137] PiezoDrive, *PDu150 – Three Channel Ultra-Low Noise 150V Piezo Driver*, (2017) `https://www.piezodrive.com/modules/pdu150-2/` (visited on 07/03/2017).